Wireless Communications and Mobile Computing

Physical Layer Security for Internet of Things

Lead Guest Editor: Ning Zhang
Guest Editors: Dajiang Chen, Feng Ye, Tong-Xing Zheng, and Zhiqing Wei

Physical Layer Security for Internet of Things

Wireless Communications and Mobile Computing

Physical Layer Security for Internet of Things

Lead Guest Editor: Ning Zhang
Guest Editors: Dajiang Chen, Feng Ye, Tong-Xing Zheng, and Zhiqing Wei

Editorial Board

Contents

Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 2627938, 2 pages
https://doi.org/10.1155/2019/2627938

Editorial

Physical Layer Security for Internet of Things

Ning Zhang,[1] **Dajiang Chen**,[2] **Feng Ye**,[3] **Tong-Xing Zheng**,[4] **and Zhiqing Wei**[5]

[1]*Department of Computing Sciences, Texas A&M University-Corpus Christi, TX, USA*
[2]*School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China*
[3]*Department of Electrical and Computer Engineering, University of Dayton, Ohio, USA*
[4]*School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China*
[5]*School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China*

Correspondence should be addressed to Ning Zhang; ning.zhang@tamucc.edu

Received 2 April 2019; Accepted 2 April 2019; Published 18 April 2019

Internet of Things (IoT) enables physical objects to sense, communicate, and perform certain actions on demand, which can facilitate a multitude of applications, such as smart home, smart city, and intelligent transportation system [1, 2]. Along with the advantages of IoT is the security issue. In IoT, the security threats are even extended from the cyberworld to cyberphysical world [3, 4]. To ensure security, the typical approach is through upper-layer cryptographic algorithms/protocols. However, they heavily rely on the availability of key management system and might be comprised as the computation power of adversaries keeps increasing [5].

As a complement, information-theoretic security can be provided by exploiting the characteristics of the physical (PHY) layer, even though adversaries have infinite computational capabilities [6–9]. With recent advances in computing, artificial intelligence, signal processing, coding, and so on, PHY security can be further enhanced to protect data and authenticate legitimate users in IoT. The interest and application of PHY security in IoT are also growing [10, 11]. The purpose of this special issue is to publish original efforts describing theoretical and practical research endeavors in the domain of PHY layer security for IoT. In this special issue, there are 13 submissions in total. After peer review, 6 papers are selected for published.

Cloud computing plays an important role in IoT. The premise of securing the cloud-based IoT context is to evaluate the security and compliance of cloud service. To this end, Xiang Li et al. propose a secure and compliant continuous assessment framework (SCCAF), to facilitate cloud service customers to select an optimal cloud service provider (CSP) which satisfies their desired security requirements. Moreover, it also enables cloud service customers to evaluate the compliance of the selected CSP in the process of using cloud services.

Xiaohui Shang et al. study the secure uplink transmission scenario in Internet of Things (IoT), where one of multiple sensors communicates with the controller aided by the cooperative relay. An energy-efficient transmission scheme (EET) is proposed, which can be suitable for the resource-constrained devices and applications in IoT communication. Moreover, the secrecy outage probability (SOP) and secure energy efficiency (SEE) of different transmission strategies are derived, which contributes to the design of energy-efficient secure transmission.

In order to ensure the security of the IoT communication system, Tao Hong et al. propose a machine learning based antenna design scheme, which can achieve directional communication from the relay tag to the receiving reader by combining patch antenna with log-periodic dual-dipole antenna (LPDA). From the simulation results, it is demonstrated that he proposed antenna design can work well in physical layer security communication, where signal-to-noise ratio of the wiretap channel is reduced, communication quality of the main channel is ensured, and information leakage is prevented.

As for securing IoT applications, Tingting Yang et al. target maritime security, where unmanned surface vessels (USV) are utilized to collect information on the sea for intelligent monitoring. To enhance the security of the unmanned

video monitoring system, an improved Hill encryption algorithm is proposed. The improved Hill encryption algorithm is integrated into the process of video compression and regulates the parameters of the encryption process according to the content of the video image. Mingsheng Cao et al. focus on wireless body area networks (WBANs), which is one of the most important IoT applications. WBANs allow patients demographics to be collected by tiny wearable and implantable sensors. These data can be used to analyze and diagnose for healthcare. In order to protect the security and privacy, Mingsheng Cao et al. propose a lightweight fine-grained search over encrypted data in WBANs, considering the limited resource of WBANs devices.

Jiefan Qiu et al. study security for over-the-air reprogramming to improve the security of reprogramming by changing the physical-level communication mode. Unidirectional Visible Light Communication (VLC) is applied to the over-the-air reprogramming and commercial off-the-shelf devices such as smartphone and sensor node are used to improve applicability. Moreover, a reprogramming approach named ReVLC is proposed. The experiment results demonstrate the effectiveness of ReVLC at the cost of extra 49.1% energy overhead compared with a traditional reprogramming approach.

With this special issue, we hope that readers will be interested in physical layer security for IoT and they find this special issue is helpful to their research.

Conflicts of Interest

Editors have no conflicts of interest to the assigned manuscripts when handling them and making decisions.

Ning Zhang
Dajiang Chen
Feng Ye
Tong-Xing Zheng
Zhiqing Wei

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] D. Zhang, Y. Qiao, L. She, R. Shen, J. Ren, and Y. Zhang, "Two time-scale resource management for green internet of things networks," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 545–556, 2019.

[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[4] F. Ye and Y. Qian, "A security architecture for networked internet of things devices," in *Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM 2017)*, pp. 1–6, Singapore, 2017.

[5] D. Chen, N. Zhang, Z. Qin et al., "S2M: a lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2017.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[7] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204–1219, 2016.

[8] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Communications Magazine*, vol. 19, no. 1, pp. 40–47, 2012.

[9] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4265–4276, 2015.

[10] L. Sun and Q. Du, "A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions," *Entropy*, vol. 20, no. 10, p. 730, 2018.

[11] A. Mukherjee, "Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 3430165, 10 pages
https://doi.org/10.1155/2019/3430165

Research Article

Secure and Smartphone-Assisted Reprogramming for Wireless Sensor Networks Based on Visible Light Communication

Jiefan Qiu,[1] **Chenglin Li**,[1] **and YueRan Li**[2]

[1]*Zhejiang University of Technology, College of Computer Science, Hangzhou, China*
[2]*National Intellectual Property Administration, Jiangsu Center, China*

Correspondence should be addressed to Jiefan Qiu; qiujiefan@zjut.edu.cn

Received 6 October 2018; Revised 15 January 2019; Accepted 24 February 2019; Published 14 March 2019

Academic Editor: Ning Zhang

During the period of over-the-air reprogramming, sensor nodes are easy to eavesdrop and even controlled by unauthorized person. That reminds us that security is key issue for over-the-air reprogramming. Most of previous studies discussed this problem from the aspect of data encryption, but give little consideration to the physical level. In this paper, we attempt to improve the security of reprogramming by changing the physical-level communication mode. We apply unidirectional Visible Light Communication (VLC) to the over-the-air reprogramming and use Commercial Off-The-Shelf device such as smartphone and sensor node to improve applicability. However, the unstable light source and low-cost light sensor make the procedure of reprogramming difficult. For this end, we put forward a novel reprogramming approach named ReVLC, which is twofold: firstly, we design a code block mechanism based on function similarity to reduce transmitting code. Secondly, we use compressing representation to optimize the Dual Header-Pulse Interval Modulation (DH-PIM) to save transmission time. The experiment results illustrate the effectiveness of ReVLC at the cost of extra 49.1% energy overhead compared with a traditional reprogramming approach.

1. Introduction

Wireless sensor networks (WSNs) systems as one kind of edge networks for IoT were always deployed in inaccessible areas for some long-term monitoring tasks. When software upgrades or even has malfunctions, the over-the-air reprogramming is the only way to online debugging or adjusting functionality without retrieving.

With respect to previous over-the-air reprogramming approaches, data transmitting is always completed by radio wave communication (RWC) and its frequency is from 10 KHz to 3000 GHz such as 2.4 GHz (Zigbee and Wi-Fi) or 800Mhz (GPRS), etc. Due to the broadcast nature of RWC, transmitting codes are vulnerable to eavesdropping and tamper. Especially, in the security-sensitive reprogramming case, some of codes or parameters are not suitable to be transmitted by broadcast mode, such as updating data encryption algorithm [1] or secret key [2, 3]. In fact, the previous studies [4–12] consider little in solving information leakage from physical level of communication. Meanwhile, Visible Light Communication (VLC) has unidirectional propagation that makes nonauthoritative person hard to eavesdrop and helps to reduce security risk. In addition, the reprogramming is applied in debugging the lost sensor node which cannot contact with other sensor nodes or sink node. For instance, our early relic-protection WSN system for Forbidden City Museum [13] was tested in laboratory and worked well. Then all nodes were locked in the glass showcase at least 3 months. Once malfunctions happen, debugging the lost node must be carried out by noncontact manner. Traditional RWC-based reprogramming approaches cannot debug the lost sensor node, but VLC-based reprogramming approach makes it possible.

For traditional VLC studies, the dedicated devices of light-signal sending and receiving are required. For example, Fan et al. improved the door control system based on VLC and the system needed a special photosensitive circuit [14]. Wang et al. designed an RGB-LED circuit to

Figure 1: Hardware interaction diagram: TelosB sensor node and smartphone.

increase the transmission rate of VLC [15]. In addition, Adiono et al. attempted to reduce the ambient light noise and develop a dedicated VLC receiver with analog filters [16]. However, the cost of dedicated light receiving device is hard to afford by low-cost sensor nodes. Thus, with respect to reprogramming such nodes, we also explore how to apply VLC in low-cost or Commercial Off-The-Shelf (COTS) devices.

Generally, ambient light sensor equipped by sensor node can sense the change of light strength and can be taken as a potential VLC signal receiver. In addition, the smartphone has potential as a VLC gateway, in the following twofold: (1) LED flashlight built-in smartphone is potential VLC signal transmitter shown in Figure 1; (2) the large memory space and transmission bandwidth guarantee caching the updating codes and forwarding them to sensor node at a little cost.

Using general hardware equipped by smartphone and low-cost sensor node will be very helpful in overcoming the barriers of applying VLC-based reprogramming to post-deployment WSN system. At the same time, using general hardware causes unstable performance of VLC, prolongs the reprogramming procedure, and even fails in reprogramming sensor node. For this end, we propose a novel reprogramming approach called ReVLC. It reduces transmission time of reprogramming from both sides: minimizing transferred data and optimizing modulation.

Previous reprogramming approaches adopted incremental strategy to minimize the transferred data. In these approaches, *delta* script [17] (consist of binary code differences and rebuilding operations) was transmitted. There approaches focus on how to improve the code similarity between the new image and old one, such as the following: Zephyr and Hermes [17, 18] improved the similarity between the old and new versions application by fixing the globe/static variable and function addresses; Li et al [19] designed an update-conscious complier to generate the new image based on the old ones and improve the similarity of both versions.

However, improving code similarity needs to change the program structure which increases difficulty on debug process. Further, such binary code differences are produced through comparing entire program image, but debugging sensor node usually is usually to fix several similar-functionality functions. Thus, we design a code block mechanism. In each block, we maintain function structure and put functionality-relevant functions in one code block. When we conduct reprogramming, these functions in same block are simultaneously replaced. By this way, only certain code blocks need to be transferred rather than entire program image.

We also present a new modulation named Compressing DH-PIM (CDH-PIM for short) based on the Dual Header-Pulse Interval Modulation (DH-PIM) [20]. DH-PIM is designed for VLC and close to the modulation efficiency of OOK. In CDH-PIM, we employ a compressing representation for repetitive bit series in modulation phase. The experiment results illustrate the transmission rate can be improved by about 17.2% compared with DH-PIM.

The rest of this paper is structured as follows: Section 2 shows relative work; Section 3 introduces the design and implementation of ReVLC; Section 4 describes experimental scenarios and evaluates our approach; and Section 5 closes with conclusion.

2. Related Work

Deluge [21] is the first and sophisticated reprogramming approach applied in wireless sensor networks, but the authors have not considered any security principle when designed it. Because Deluge needs to transmit the entire program image with a long period of reprogramming, sensor nodes are vulnerable to attack. Thus, the early secure reprogramming studies [3, 4] focus on the extensions to Deluge and guarantee data integrity and authenticity. For example, Sluice [3] employs signature and cryptographic hash function to generate the hash image of program image as authentication. It also follows Deluge to divide program image into pages and each page contains the hash image of next pages. Hyun et al [4] presented Seluge to optimize the transmission overhead for Markle hash tree and reduce the page propagation delays.

With secure techniques ongoing, researchers pay more attention to the general attack and excessive security overheads of reprogramming. Park et al [5] proposed a lost packet recovering method by supplementary hash scheme and page digest scheme. DART [6] is proposed by Dong et al. who used time-based authentication to defend pollution attacks and it needs time asymmetry which brings up additional delay. In Sreluge protocol [7], author solved the problem of authenticating data packets by encoded packet using random linear codes. Dong et al. [8] have presented two filtering method to protect from DoS attacks by signature verification. Tan et al. [9] proposed a reprogramming protocol which integrates confidentiality and Dos-attack-resistance countermeasures suitable to WSN. Kim et al. [10] designed three source authentication reprogramming schemes which support dynamic packet size. LDSCD [11]

is a social role-based distributed reprogramming framework against DoS attack and supports multiple authorized tenants. Yang et al. [12] considered excessive overheads for security mechanism and proposed a security enhancement reprogramming approach based on a hierarchical hash tree.

Above approaches considered the security problem of reprogramming by modifying upper-layer software and were not still to totally prevent from eavesdrops due to the broadcast nature of RWC. In this paper, we attempt to change physical-level communication mode and improve the security of reprogramming.

3. Design and Implementation of ReVLC

In this section, we firstly present code block mechanism based on function similarity and then introduce CDH-PIM applied in ReVLC. The former reduces the transmitting data of reprograming and the latter optimizes VLC modulation to make it applied in general devices. At last, we also describe the implementation of ReVLC.

3.1. Code Block Mechanism. The early RWC-based reprogramming approaches [21, 22] need to transfer whole program imager, but the size of program image is clearly overlarge for VLC-based reprogramming. In fact, the bugs exist in several functionality-relevant functions. Thus, the problem functions should be fixed not whole program image.

ReVLC provides a mechanism to divide the program image into several code blocks according into functionality. That means putting the functionality-relevant functions in one code block and transferring corresponding code blocks instead of whole image.

In our previous work [23], we have found that the functionality-relevant functions can be described by the function similarity between independent functions. The function similarity is defined based on an observation that the modification of function has unidirectionality, namely, that caller function will be changed with high possibility if the callee function has been changed; the opposite situation rarely happens. Thus, we firstly defining function similarity degree (FSD) to measure the function similarity based on the collaborative filtering algorithm. Given functions u and v, $N(u)$ and $N(v)$ are, respectively, the callee function in u and v. The FSD S_{uv} between u and v can be described by Jaccard formula:

$$s_{uv} = \frac{|N(u) \cap N(v)|}{|N(u) \cup N(v)|} \tag{1}$$

After obtaining each S_{uv} between two functions, we calculate the whole function similarity degree (S) of code block with different weight, as follows:

$$S(f_1, f_2, \ldots, f_i) = \sum_{u=1}^{i} \sum_{v=1}^{i} \beta_{uv} s_{uv}$$
$$\beta_{uv} = \frac{1}{size(u) * size(v)} \tag{2}$$

where β_{uv} is weighted value, which is inversely proportional to the size of function u and v. It ensures that if u and v own smaller size with a high FSD, the whole FSD of code block is high; conversely, if u and v own large size with a high FSD, the whole FSD of code block should be reduced. By calculating the FSD, the program image can be divided into several code blocks.

On the other hand, each code blocks can be migrated to several sensor nodes with different address. The new address of each function is uncertain before reprogramming. If modifying each call instruction according new address, the rebuilding overhead is large and not afforded by sensor node. To simplify this process, we have adopted a register relative addressing to invoke each function in RePage.

In each code block, the `call` instruction must be modified to the register relative addressing and the real entry address of callee function is saved in Function Location Table (FLT) shown in Figure 2. In addition, a hash table (HT) needs maintaining in sensor nodes. The HT contains the real entry addresses of each function and locates in high address of program flash. FLT is fixed in the tail of each code block. It saves hash values and the offset address of each function relative to the code block.

The hash value is generated by hash function *Hash*(fun_name) where function name is taken as hash key. When a code block adds new function, FLT needs correspondingly adding one new item and grows forward the low address like stack behavior.

When a code blocks arrive in a sensor node, the runtime system would load code block with following 3 steps:

(1) Assign a new address to insert the code blocks in program flash and this address is the base address of functions contained in the new code block.

(2) Modify the first `mov` instruction located in the head of each function BY the begin address of HT in local node.

(3) Modify HT according into the hash value saved in FLT and the begin address of HT using the new function addresses, which is figured out by offset+base address.

Before calling the function, the begin address of HT should be assigned to a certain register, for instance, using register *r5* saves the begin address (0xBC00) illustrated in Figure 2. Therefore, in step (2), we must reassign *r5* by `mov` instruction located in the head of each function of new code block.

When a caller function call a callee function based on the register relative addressing, register *r5* combining with relative address which is hash value (0x0054) and point to the item of the HT which save the real entry address of function. Finally, realize the function invoking process.

In Section 3.3, we also discuss that modify `mov` instruction which reassigns *r*5 and the address as parts of each call instruction using hash value. Both of modifications happen in precompiling phase. Certainly, they are transparent to developer or networks owner.

3.2. Compressing Dual Header-Pulse Interval Modulation. Different from RWC, signal modulation of VLC depends on switching LED's state. The LED switch rate is faster than fluorescent and filament lamp, so smartphone equipped

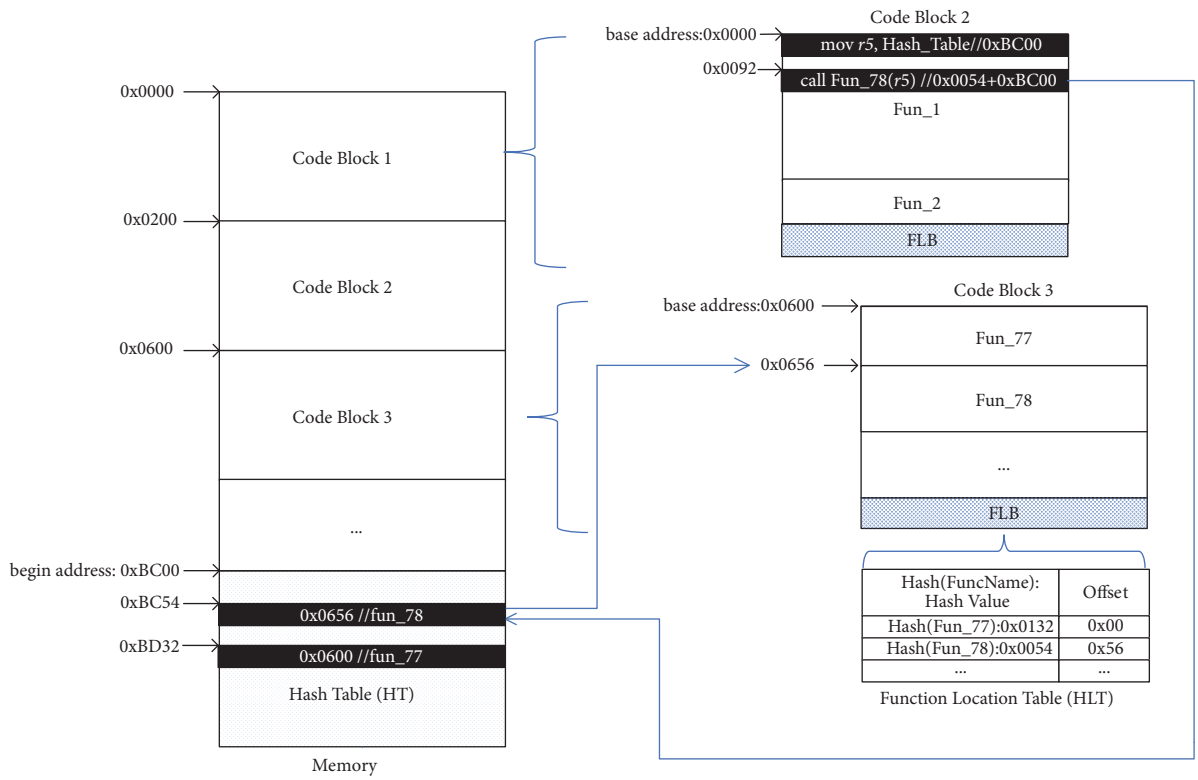


FIGURE 2: Memory layout and function calling process: the entry address of Fun_78 located in code block3 is 0x0656H and saved in hash table with address 0xBC54H. Invoking Fun_78 needs to obtain the hash table address (0xBC54), and then using function entry address (0x0656H) to complete invoking process.

with LED flashlight is a potential light-signal transmitter. However, the dedicated light-signal receivers are usually complex and hard to afford by low-cost sensor nodes. In order to realize VLC between sensor node and smartphone, we try to employ the ambient light sensor built-in sensor node as light-signal receiver.

However, using the ambient light sensor has an unappealing communication performance, because these sensors have a long response latency and opening time. Both of parameters decide the minimum detectable pulse width. We define the double width of minimum detectable pulse width as the one time slot t_r.

In addition, the reprogramming is a bursting procedure. Namely, several code blocks transmit within a short period. Above problems make it difficult that apply directly VLC to over-the-air reprograming.

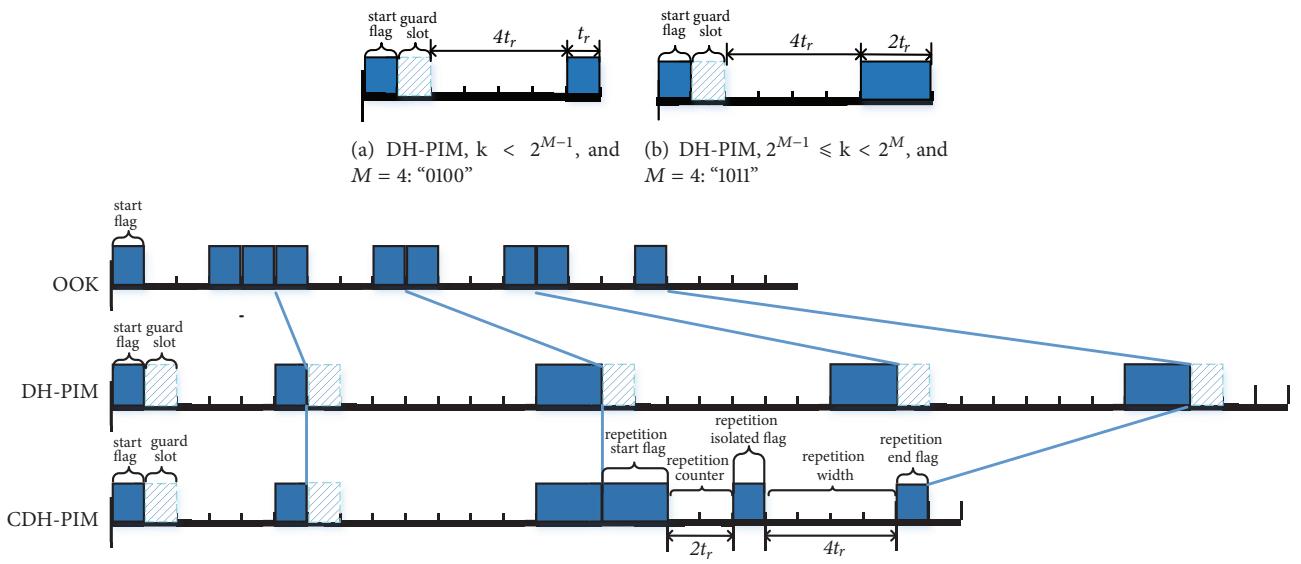
Based on large numbers of experiments, we found a lot of continuously repetitive parts (such as "1010 1010 1010") exist in the bit series of code block. This find lets us consider compressing the continuously repetitive parts and propose a Compressing DH-PIM (Dual Header-Pulse Interval Modulation). The CDH-PIM, for short, divides the continuous bit series to nonrepetitive and repetitive parts according to content.

For nonrepetitive parts, CDH-PIM adopts DH-PIM designed for VLC [20]. DH-PIM is an anisochronous pulse time modulation in which data are encoded as discrete time slots between adjacent pulses. A symbol which encodes M bits of data is represented by k slots of low power and followed by one pulse of constant power, where $0 \leqslant k \leqslant L/2\text{-}1$ and $L = 2^M$. The pulse of constant power will last t_r or $2*t_r$ for two numbers which are radix-minus-one complement. For example, the number "0100" has 4 slots of low power and 1 slot pulse of constant power. The number "1011" is radix-minus-one complement of "0100" and has 4 slots of low power and 2 slots pulse of constant power.

For repetitive parts, CDH-PIM adopts a compressing representation to reduce the number of slots. The repetitive part can be represented by three parts: first nonrepetition bits, repetition counter, and width. The latter two parts need special symbols to mark.

In practice, given M=4, the one slot pulse and two slot pulse were used to represent for $k<2^{M-1}$ and $2^{M-1} \leqslant k < 2^M$ shown in Figures 3(a) and 3(b). It needs 3 repetition flags in order to mark and identify the repetition counter and width as shown in Figure 3(c). The successive 2 slots pulses are repetition start flag and followed by the normal DH-PIM's 1 slot pulse and taken as start flag for the repetition counter. The next one pulse is repetition isolated flag to divide the repetition counter and width. The last one slot pulse is the repetition end flag of repetition width. The repetition counter and width are represented by the number of slots of zero power.

As illustrated in Figure 3(c), to represent the repetition part, it needs 4 slots pulses and 6 slots of zero power for expression, compared with 4 slots pulses and 14 slots of zero



(a) DH-PIM, k < 2^{M-1}, and M = 4: "0100"

(b) DH-PIM, $2^{M-1} \leqslant$ k < 2^M, and M = 4: "1011"

(c) Three modulations comparison. bit series: "0011 1001 1001 1001"

Figure 3: Modulation comparison: (1) OOK modulation; (2) Dual Header-Pulse Interval Modulation; (3) Compressing Dual Header-Pulse Interval Modulation.

Table 1: Function table.

Fun Name	Fun Size	Calling Relationship
Fun_2	96 B	Fun_78,Fun_1,...

power of DH-PIM. The transmission time reduces 44%. In such case, the 3 repetition flags need extra 4 slot pulse.

It should be noted that some cases cannot be applied compressing representation. For example, a bit series "0000 0000 0000" is modulated by DH-IPM and only needs 3 pulses and 3 slots of zero power compared with using CDH-PIM with 5 pulses and 7 slots of zero power. Thus, to deal with the repetitive part, the extra cost caused by tree types of repetition flags needs to be considered before modulation.

3.3. Implementation of ReVLC. We run ReVLC on a popular sensor network OS TinyOS. The running phase of ReVLC can be divided to three parts: the compilation phase (compile the program image), transmitting phase (transmitting code block by VLC), and the loading phase (deploy code block).

As shown in Figure 4(a), compilation phase occurs in smartphone or cloud. In ReVLC, it needs to perform twice compilations for code block. In the first compilation, we make a modification on dead code elimination of TinyOS and keep all the functions existing in image program file [24]. Then, establish the function table through reading the symbol table of executable (.exe). The function table comprises function name, function size, and the calling relationship which records all callee functions by current function. The function table is as shown in Table 1.

The function table is generated after the first compilation. Using the calling relationship, the function similarity degree (FSD) between functions can be calculated and saved in function table. In terms of FSD, ReVLC readjusts all positions of functions and puts functions into each code block. It also reserves space in each code block for FLT.

In the second compilation, the hash values are figured out by *Hash*(fun_name). The hash values are filled into the FLT. In the precompilation phase, we modify the addressing mode of calling function and add the register assignment instructions (`mov` instruction) in the head of each function. The source file needs compiling again according to the new readjusted function addresses.

Figure 4(b) shows transmitting and loading phase. Firstly, ReVLC figures out all the repetitive parts in the bit series of code block. Then evaluate and compare the cost of using compressing representation with not using. Then the modulated bit series are packaged into one or several frames and transmitted by VLC. In target sensor nodes, the transmitted bit series are demodulated.

Once code block arrives in sensor node, runtime system provides new spaces for the new code block. Then, it rewrites the local hash table in terms of the FLT of new code block and modifies the source operand (The begin address of HT) of the `mov` instruction in each function of the new code block. Finally, the runtime system starts software reboot procedure to restart target node.

4. Evaluation

In this section, we conduct a series of experiments in continuous updating cases. We firstly introduce the experiment methodology and then evaluate ReVLC.

4.1. Experiment Methodology. We implement ReVLC based on a Samsung N7100 smartphone powered by Android and TelosB sensor node [25] installed TinyOS-2.x. As shown in Figure 5, TelosB node equips with 2.4 GHz Zigbee RF

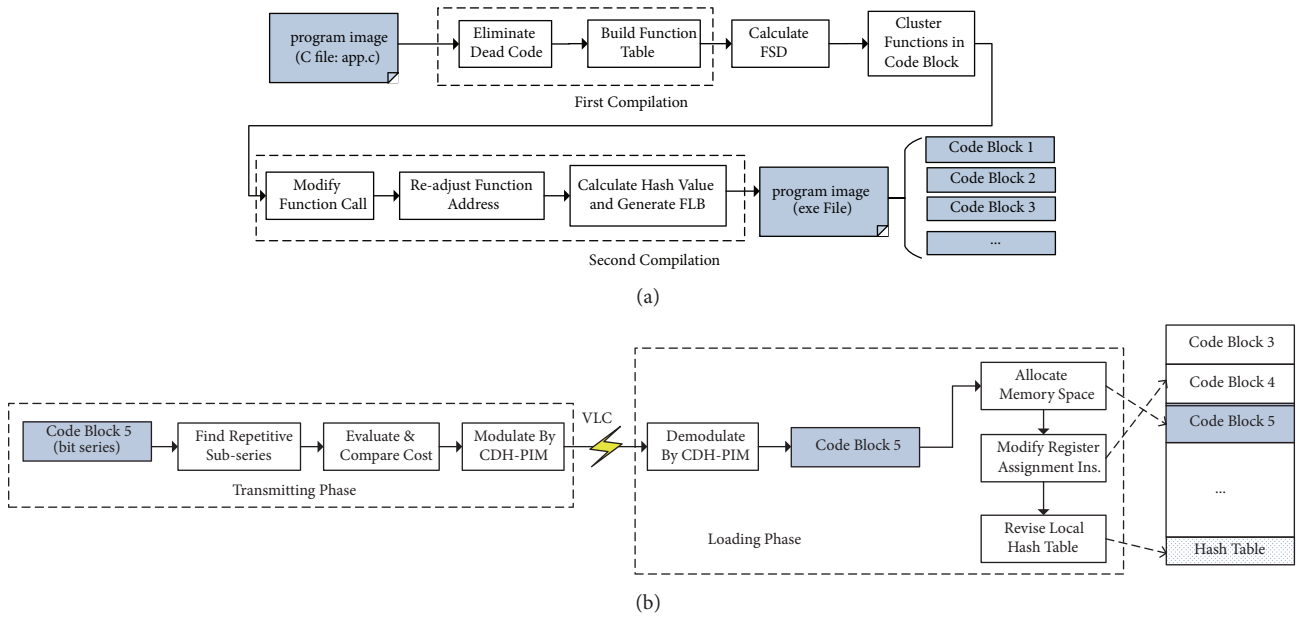


Figure 4: Implementation of ReVLC: (a) compilation phase; (b) transmitting and loading phase.

Figure 5: Sensor node and current-monitoring circuit: (a) TelosB sensor node; (b) packaged TelosB with light hole; (c) current-monitoring circuit with MAX9928.

transceiver CC2420, a 16-bit MCU MSP430F1611 (10kB RAM and 48kB program flash), and an ambient light sensor TSL2561. We evaluate the energy overhead and measure current change by a dedicated current-monitoring circuit equipped current-sense amplifiers MAX9928 [26] as shown in Figure 5(c).

4.1.1. Experimental Basic Setup

(1) The sensor node memory space: 1kB program flash (address: 0xFBFF-0xFFFF) for HT and 13kB program flash (address: 0xC708 to 0xFBFE) for ReVLC's runtime system.

(2) The max size of frame is 2048 bits, and size of header of each package is 30 bits, including start flag (2 bits), frame size (20 bits), and code block ID (8 bits).

(3) The size of code block is 256 bytes. FLT is located at the end of each code block. Each item of FLT is 5 bytes with hash value (3 bytes) and location information (2 bytes).

Updating Case Setup. We describe eight updating cases in the real world. In the first updating case, the target sensor node installed a standard routines program named Oscilloscope which is contained in TinyOS application library. The other five versions of programs are named EasiRoute (version from v0.1 to v0.3). They are developed for our relic-protection WSN system which has been deployed in the Forbidden Palace Museum [13]. Each version means a major upgrade. As shown in Figure 6, six programs are continuously updated according to an alphabetical order:

Updating Case A. Oscilloscope executes a standard data collection program. By adding a routing functionality, we update it to EasiRoute_v0. 1.

Updating Case B. Update EasiRoute from v0.1 to v0.11. After this update, a sensing-data storing module is added, and it realizes storing data in external flash chip.

Updating Case C. Directly update Oscilloscope to v0.11, and add routing and storing modules in target node.

Table 2: Comparison of transmitting data among ReVLC, RePage, and Tiny Module-link (Bytes).

	Case A	Case B	Case C	Case D	Case E	Case F	Case G	Case H
Tiny Module-link	876	225	656	296	1844	52	2678	2924
RePage	924	368	674	312	1766	52	2536	3014
ReVLC	1024	512	768	512	1536	256	2348	3328

Table 3: Comparison of memory space among ReVLC, RePage, and Tiny Module-link (Bytes).

		Case A	Case B	Case C	Case D	Case E	Case F	Case G	Case H
Tiny Module-link	Program Flash	14758	14796	15036	15720	15456	15456	18356	18704
	RAM	——	——	——	——	——	——	——	——
RePage	Program Flash	12256	12256	12256	12256	12256	12256	12256	12256
	RAM	5120	5120	5632	5632	5632	6144	6144	6144
ReVLC	Program Flash	13558	13558	13558	13558	13558	13558	13558	13558
	RAM	——	——	——	——	——	——	——	——

Updating Case D. Update museum monitoring program from v0.11 to v0.18. After the update, a bug will be fixed. This bug leads that sensor node to send data to sink node too often when museum is powered off at night.

Updating Case E. Update v0.11 to v0.21. We add a sleep mechanism to balance load based on the battery energy remaining.

Updating Case F. Update v0.18 to v0.21. The new version will remove the sensing-relevant functions from the node. It only retains routing function and forwards data from other ones.

Updating Case G. Update v0.18 to v0.3. After this update, node will install the UDP protocol which supports the fact that users directly interact with the nodes through web browser.

Updating Case H. Update v0.21 to v0.3.

We will test the performance of ReVLC in three aspects: transmission and memory overhead, rebuilding overhead, and the performance of VLC applied in reprogramming.

4.2. Transmission and Memory Overhead. Different from the incremental reprogramming approaches [17–19, 23, 27], transmitting data of ReVLC only consist of code blocks. We compare ReVLC with other incremental reprograming approaches such as RePage [23] and Tiny Module-link [27]. In RePage, program image is divided into each function page like the code block and modifies each page according to *delta* script. Tiny Module-link directly modifies function codes, but the updated functions need storing in tail of code segment (.text segment).

Table 2 gives details about transmitting data under 6 cases. Clearly, in six cases, the RePage and Tiny Module-link have advantage over ReVLC, because both of approaches can modify the image using smaller-size *delta* script.

For example, in case F, the *delta* script is mainly comprised by rebuilding operations to remove the sensing-relevant functions about RePage and Tiny Module-link. ReVLC still

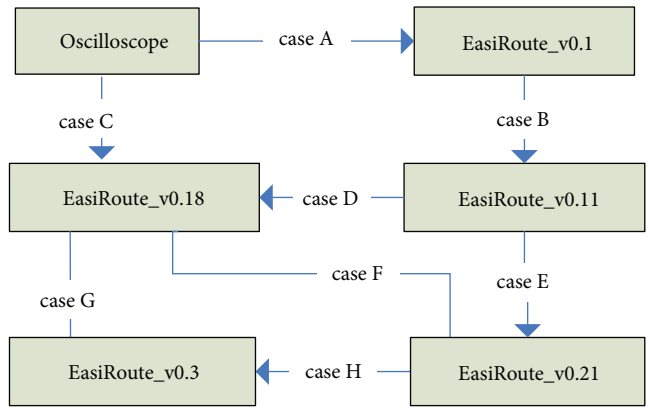


Figure 6: Roadmap of continuously updating.

transfers one code block at four times over both. But case C and case G are special. In both cases, the modified processes are complex. It means that several functions were changed, and *delta* script contains about 430 bytes of rebuilding operations. ReVLC only transmits new code blocks without these operations, and thus, its transmitting data are conversely less than the two others. Finally, the average of transmitting data of ReVLC is 7.12% and 6.2% higher than Tiny Module-link and RePage.

Memory overhead is mainly brought up by extra codes and the runtime system. As shown in Table 3, three runtime systems occupy 12256B, 13558B, and 14124B program flash space with respect to RePage, ReVLC, and Tiny Module-link. ReVLC's runtime system needs a demodulation module for CDH-PIM. Therefore, the size of ReVLC's runtime system is larger than RePage. In addition, due to writing external flash, the runtime system of Tiny Module-link needs 1.4 kB and its size is largest among three approaches.

With respect to extra codes, Tiny Module-link puts the size-increasing functions in tail of code segment (.text segment) without RAM participation, so the extra codes will be increasingly stored in program flash. On the other hands, RePage caches the frequently updating function pages

in low-power RAM to reduce rebuilding energy, so with reprograming ongoing, the cache area in RAM grows until fulling cache (6144 bytes). Conversely, the ReVLC directly replaces the old code block with new one stored in flash program. Therefore, there is no extra codes existing in RAM or program flash.

4.3. Rebuilding Overhead. The energy overhead of over-the-air reprogramming mainly comes from the code transmission and program rebuilding when read/write memory [28]. In fact, rebuilding overhead in volatile memory (such as RAM) is far less than that the nonvolatile memory (such as program flash). Take the TelosB nodes as example and the energy overhead of writing and reading (wt/rd for short) operations on the program flash is 14.6 times than on RAM. Therefore, when studying rebuilding overhead of over-the-air reprogramming, we focus on the number of wt/rd operations on program flash.

We compare ReVLC with RePage [23] under eight continuously updating scenarios. Like ReVLC, RePage adopts a paging mechanism to cluster the similar function, while it, as one incremental reprograming approach, only transfers the *delta* script between old and new function pages. RePage needs to store new page in cache (RAM) or program flash. Thus, in RePage, it necessary to write program flash to replace pages and read program flash to cache page in RAM or rebuild new page. Meanwhile, ReVLC transfers entire cold block and directly writes new block into program flash, so it is unnecessary to read program flash.

Figure 7 gives the number of wt/rd program flashes. In case A-case D, the performance of RePage is closed to ReVLC and the difference of wt/rd operations between RePage and ReVLC is 9.8%, because of no replacement happening. In case E, one-function pages are replaced in RePage. That means one page needs writing into program flash and the other one needs to reading from program flash. Such exchanging 512 bytes of function page brings up increasing 31.9% rebuilding overhead than ReVLC. In case F, using RePage, although only inserting or revising operations are fewest in all cases, the deleting operations lead to move codes to new position.

Meanwhile, in ReVLC, it only overwrites the old code blocks. In case G and H, several functions are inserted in program due to adding UDP protocol. In RePage, several function pages saved in program flash are cached in RAM and 2 pages replaced from cache. Finally, the wt/rd operations of RePage exceed 4.5 kB compared with 2.3kB and 3.3kB using ReVLC in case G and case H.

4.4. Performance of VLC Applied in Over-the-Air Reprogramming. In ReVLC, we optimize a current DH-PIM by bit-level compressing representation and propose Compressing DH-PIM (CDH-PIM). With respect to sensing hardware, the ambient light sensor TSL2561 is equipped by sensor nodes. Its minimum detectable pulse width is about 10ms. That means only the light pulse exceeds 10ms, and the sensor can stably measure light strength.

Therefore, the slots tr are set to 20ms and M=4 of CDH-PIM. Figures 8 and 9 show the completion time and transmission rate with DH-PIM and CDH-PIM in eight cases. The average transmission rate of CDH-PIM is 54.8 bit/s compared with 45.4 bit/s of DH-PIM. The completion time of CDH-PIM also reduces 16.3% than DH-PIM. This also suggests that a lot of bit continuous repetitions exist in transferred code blocks.

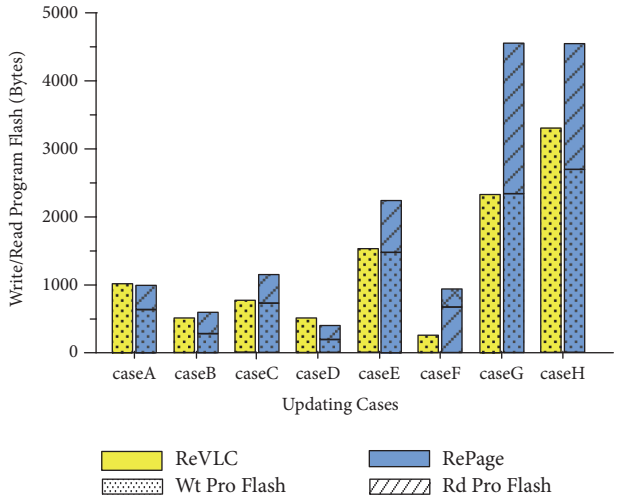


Figure 7: Rebuilding overhead.

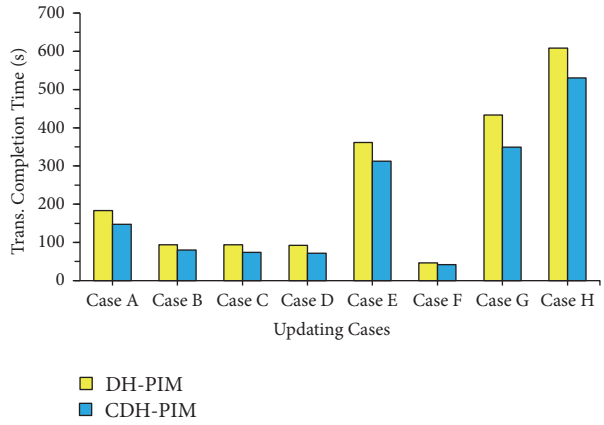


Figure 8: Transmission completion time (s).

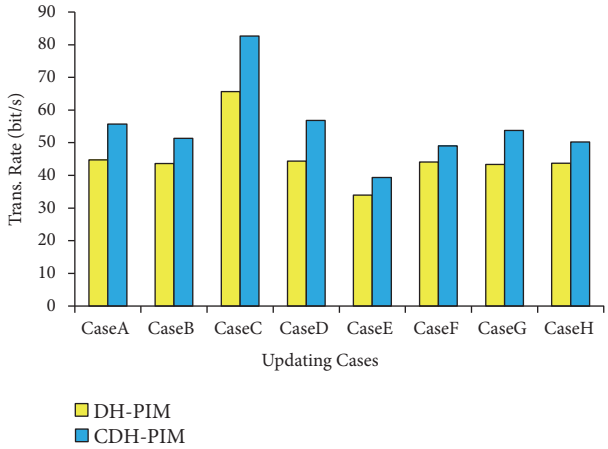


Figure 9: Transmission rate (bit/s).

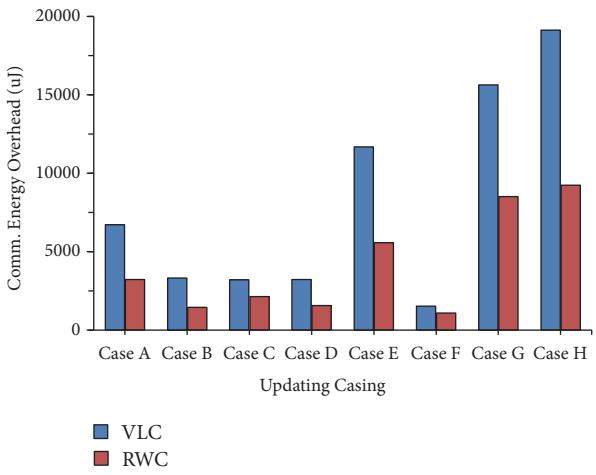


Figure 10: Communication energy overhead (uJ).

Further, we compare VLC with RWC based on energy overhead which is important for battery-power sensor nodes. We conduct a reprogramming procedure on one sensor node and then send block codes from sink node by RWC and smartphone by VLC, respectively. Figure 10 gives the energy overhead of the sensor node using VLC and RWC. The energy overhead is measured by current-monitoring circuit. The energy overhead of VLC mainly comes from turning on TSL2561 during transmission period. Obviously, the power of ambient light sensor is higher than the traditional RF transceiver CC2420. The high-power light sensor leads to the fact that the average energy overhead of VLC increases 49.1% than RWC. However, in most of security-sensitive cases, this energy overhead increasing is acceptable. In addition, given that lost sensor node is or offline from network, the ReVLC may be only viable reprogramming solution to fix sensor node.

5. Conclusion

Most of current reprogramming approaches solve the security problem in upper-level software such as adding complex security mechanism. In this paper, we attempt to reduce the security risk by changing the physical-level communication mode. For this end, we propose a VLC-based reprogramming approach, ReVLC applied in resource-limited sensor node. In this approach, we directly use low-cost and general sensor nodes without hardware modification and a CTOS smartphone as VLC gateway to save and forward codes. Meanwhile, using the ambient light sensor equipped by sensor node as signal receiver leads to unappealing transmission performance. So, in ReVLC, we propose a code block mechanism to minimize transferred data and CDH-PIM with compressing representation to optimize modulation of VLC. The experiment results prove the availability of ReVLC.

In future work, we will continuously study the VLC modulation from the more compressing representation and also introduce the probability coding such as Huffman Coding into modulation.

Data Availability

Figures 7–10 and Tables 2-3 which are used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research work is supported by China Natural Science Foundation (NSF) under Grant no. 61502427 and by the Zhejiang Provincial Natural Science Foundation of China under Grant no. LY16F020034.

References

[1] Y. C. Luo, J. G. Wu, Z. K. Zhang, W. J. Shi, and Y. Q. Miu, "Online algorithm for secure task offloading in dynamic networks," in *Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*, China, 2017.

[2] Y. Rao, J. Wang, R. Tian, and F. Zhu, "Dynamic updating based key management algorithm for wireless sensor networks," in *Proceedings of the 2011 International Conference on Wireless Communications and Signal Processing, WCSP 2011*, China, November 2011.

[3] P. E. Lanigan, R. Gandhi, and P. Narasimhan, "Sluice: secure dissemination of code updates in sensor networks," in *Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS '06)*, July 2006.

[4] S. Hyun, P. Ning, A. Liu, and W. Du, "Seluge: Secure and DoS-resistant code dissemination in wireless sensor networks," in *Proceedings of the 2008 International Conference on Information Processing in Sensor Networks, IPSN 2008*, pp. 445–456, April 2008.

[5] K. Park, J. H. Lee, T. Y. Kwon, and J. Song, "Secure dynamic network reprogramming using supplementary hash in wireless sensor networks," in *Proceedings of the Fourth International Conference on Ubiquitous Intelligence and Computing*, pp. 653–662, Hong Kong, 2007.

[6] J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defenses against pollution attacks in wireless network coding," *ACM Transactions on Information and System Security*, vol. 14, no. 1, 2011.

[7] Y. W. Law, Y. Zhang, J. Jin, M. Palaniswami, and P. Havinga, "Secure rateless deluge: pollution-resistant reprogramming and data dissemination for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, Article ID 685219, 22 pages, 2011.

[8] Q. Dong, D. Liu, and P. Ning, "Pre-authentication filters: Providing DoS resistance for signature-based broadcast authentication in sensor networks," in *Proceedings of the WiSec'08: 1st ACM Conference on Wireless Network Security*, pp. 2–13, USA, April 2008.

[9] H. Tan, D. Ostry, J. Zic, and S. Jha, "A confidential and DoS-resistant multi-hop code dissemination protocol for Wireless Sensor Networks," in *Proceedings of the 2nd ACM Conference on*

Wireless Network Security, WiSec'09, pp. 245–252, Switzerland, March 2009.

[10] D. Kim, D. Kim, and S. An, "Source authentication for code dissemination supporting dynamic packet size in wireless sensor networks," *Sensors*, vol. 16, no. 7, 2016.

[11] M. Xie, U. Bhanja, J. Shao, G. Zhang, and G. Wei, "LDSCD: A loss and DoS resistant secure code dissemination algorithm supporting multiple authorized tenants," *Information Sciences*, vol. 420, pp. 37–48, 2017.

[12] L. Yang, S. Li, Z. Xiong, and M. Qiu, "HHT-based security enhancement approach with low overhead for coding-based reprogramming protocols in wireless sensor networks," *Journal of Signal Processing Systems*, vol. 89, no. 1, pp. 13–25, 2017.

[13] D. Li, W. Liu, and L. Cui, "EasiDesign: An improved ant colony algorithm for sensor deployment in real sensor network system," in *Proceedings of the 53rd IEEE Global Communications Conference, GLOBECOM 2010*, USA, December 2010.

[14] L. Fan, Q. Liu, C. Jiang et al., "Visible light communication using the flash light LED of the smart phone as a light source and its application in the access control system," in *Proceedings of the 2016 IEEE MTT-S International Wireless Symposium, IWS 2016*, China, March 2016.

[15] Y. Wang and N. Chi, "A high-speed bi-directional visible light communication system based on RGB-LED," *China Communications*, vol. 11, no. 3, pp. 40–44, 2014.

[16] T. Adiono, A. Pradana, R. V. W. Putra, and S. Fuada, "Analog filters design in VLC analog front-end receiver for reducing indoor ambient light noise," in *Proceedings of the 2016 IEEE Asia Pacific Conference on Circuits and Systems, APCCAS 2016*, pp. 581–584, Republic of Korea, October 2016.

[17] R. K. Panta, S. Bagchi, and S. P. Midkiff, "Zephyr: efficient incremental reprogramming of sensor nodes using function call indirections and difference computation," in *Proceedings of USENIX Annual Technical Conference*, 2009.

[18] R. K. Panta and S. Bagchi, "Hermes: Fast and energy efficient incremental code updates for wireless sensor networks," in *Proceedings of the 28th Conference on Computer Communications, IEEE INFOCOM '09*, pp. 639–647, Brazil, April 2009.

[19] W. Li, Y. Zhang, J. Yang, and J. Zheng, "UCC: Update-conscious compilation for energy efficiency in wireless sensor networks," in *Proceedings of the PLDI'07: 2007 ACM SIGPLAN Conference on Programming Language Design and Implementation*, pp. 383–393, USA, June 2007.

[20] N. M. Aldibbiat, Z. Ghassemlooy, and R. McLaughlin, "Error performance of dual header pulse interval modulation (DH-PIM) in optical wireless communications," *IEE Proceedings—Optoelectronics*, vol. 148, no. 2, pp. 91–96, 2001.

[21] J. W. Hui and D. Culler, "The dynamic behavior of a data dissemination protocol for network programming at scale," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys'04)*, pp. 81–94, ACM, November 2004.

[22] R. K. Panta, I. Khalil, and S. Bagchi, "Stream: Low overhead wireless reprogramming for sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications (IEEE INFOCOM '07)*, pp. 928–936, USA, May 2007.

[23] J. Qiu, S. Li, and B. Cao, "RePage: A novel over-air reprogramming approach based on paging mechanism applied in fog computing," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[24] W. Dong, Y. Liu, C. Chen, L. Gu, and X. Wu, "Elon: Enabling efficient and long-term reprogramming for wireless sensor networks," *ACM Transactions on Embedded Computing Systems*, vol. 13, no. 4, article no. 77, 2014.

[25] J. Polastre, R. Szewczyk, and D. Culler, "Telos: enabling ultra-low power wireless research," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 364–369, April 2005.

[26] MAX9928 introduction, available in: http://www.maximintegrated.com/datasheet/index.mvp/id/5753.

[27] S.-K. Kim, J.-H. Lee, K. Hur, K.-I. Hwang, and D.-S. Eom, "Tiny module-linking for energy-efficient reprogramming in wireless sensor networks," *IEEE Transactions on Consumer Electronics*, vol. 55, no. 4, pp. 1914–1920, 2009.

[28] K. Lorincz, B.-R. Chen, and G. W. Challen, "Mercury: a wearable sensor network platform for high-fidelity motion analysis," in *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys '09)*, pp. 183–196, ACM, November 2009.

Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 9340808, 12 pages
https://doi.org/10.1155/2019/9340808

Research Article

A Lightweight Fine-Grained Search Scheme over Encrypted Data in Cloud-Assisted Wireless Body Area Networks

Mingsheng Cao,[1] **Luhan Wang**,[1] **Zhiguang Qin**,[1] **and Chunwei Lou**[2]

[1] *School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China*
[2] *University of Electronic Science and Technology of China, Chengdu 611731, China*

Correspondence should be addressed to Zhiguang Qin; qinzg@uestc.edu.cn

Received 3 October 2018; Revised 20 November 2018; Accepted 4 December 2018; Published 1 January 2019

Guest Editor: Feng Ye

The wireless body area networks (WBANs) have emerged as a highly promising technology that allows patients' demographics to be collected by tiny wearable and implantable sensors. These data can be used to analyze and diagnose to improve the healthcare quality of patients. However, security and privacy preserving of the collected data is a major challenge on resource-limited WBANs devices and the urgent need for fine-grained search and lightweight access. To resolve these issues, in this paper, we propose a lightweight fine-grained search over encrypted data in WBANs by employing ciphertext policy attribute based encryption and searchable encryption technologies, of which the proposed scheme can provide resource-constraint end users with fine-grained keyword search and lightweight access simultaneously. We also formally define its security and prove that it is secure against both chosen plaintext attack and chosen keyword attack. Finally, we make a performance evaluation to demonstrate that our scheme is much more efficient and practical than the other related schemes, which makes the scheme more suitable for the real-world applications.

1. Introduction

With the rapid advancement of wireless communication technology and wearable medical sensors, medical area will be largely revolutionized by the emergence of wireless body area networks (WBANs) as a highly innovative technique [1, 2]. A typical WBAN consists of a controller and a number of wearable and implantable medical sensors. These sensors are exploited to place on human body for continuously monitoring physiological symptoms or collecting related body parameters. The aggregated data via wireless networks (like Bluetooth, Zigbee, Wifi, or GPRS) are finally transferred from one mobile terminal (such as a smart phone or a PAD) to cloud servers for remotely storing and accessing. With WBANs, two great benefits can be rendered for patients and healthcare providers. One hand is that medical patient's conditions can be remotely diagnosed instead of being measured in the traditional face-to-face way. For another one, healthcare provider can access medical records remotely to provide medical treatment in real time. Although great potential in improving healthcare quality has been shown, security and privacy protection of data collected from WBANs remains to be a major concern [3, 4], which hampers the far-ranging application of WBANs since the data stored on servers are no longer out of physical control by data owners.

To protect the data privacy, a frequently adopted method is to encrypt the medical data prior to transmitting them to servers; however, data encryption makes information retrieval over the encrypted data greatly difficult. In addition, a naive solution for data users is to download-then-decipher all the ciphertexts locally since it incurs too much computational overhead and wastes considerable bandwidth resources. Accordingly, preserving the confidentiality of medical data and achieving efficient data retrieval simultaneously are of significant importance in cloud-assisted WBANs scenarios. To resolve the issue of efficient searching over the encrypted medical data, the searchable encryption (SE) technique [5, 6], which allows users to delegate their searchability to cloud server for securely and selectively retrieving the encrypted medical data of interest, has been extensively researched. At present, a lot of work focusing on SE has been explored to gain various searching functionalities like single

keyword search [7, 8], multikeyword search [9, 10], fuzzy keyword search [11, 12], and so on. Although much attention in SE technology has been attracted in both academical and industrial fields, it is still unsuitable for WBANs as patients commonly desire that their medical data could be shareable and accessible by different data users (e.g., government agencies, healthcare providers, medical researchers, and insurance underwriters). To furnish access control with fine-granularity over medical data in SE solutions, ciphertext policy attribute based keyword search (CP-ABKS) is proposed [13, 14]. In a CP-ABKS scheme, data users can decipher the ciphertexts of interest on the premise that the attributes match the access policy attached to the ciphertexts and meanwhile the submitted trapdoors satisfy the keyword indexes.

Despite the fact that both fine-grained access control and search functionalities can be implemented in CP-ABKS, the computational and storage costs of much of existing CP-ABKS schemes increase linearly with the complexity of access policies, which severely impedes the use of resource-limited mobile devices. Consequently, in practice, it is greatly essential to provide lightweight operations for data users.

In this paper, we devise a novelly lightweight fine-grained keyword search over encrypted medical data in WBANs. With our proposed scheme, flexible and fine-grained access control in multiple data user setting and lightweight keyword search over the encrypted medical data can be achieved. Furthermore, lightweight computational and storage overhead on end users throughout our scheme can also be gained as our primary design objective. To sum up, the main contributions are provided below:

(i) Fine-grained keyword search. Our proposed scheme can achieve one-to-many encryption instead of one-to-one encryption and enforce fine-grained access control over the medical data such that the medical data can only be searched and accessed if the attributes of data user match the access policy.

(ii) Lightweight search algorithm. Our proposed scheme can support data user in retrieving the ciphertexts of interest according to the queried keyword. To be specific, after receiving the trapdoor from the data user, the cloud server performs a search algorithm to search the encrypted medical data. During the searching process, only three pairing computations are needed for the cloud server to compete a searching operation.

(iii) Lightweight decryption and verification. In our proposed scheme, the great majority of decryption operations are offloaded to the cloud server such that considerable decryption overhead of an end user is relieved and only an exponentiation is required by the end user. Further, the end user can validate that the transformed ciphertext completed by the cloud server is correct.

(iv) Security and practicability. The detailed security proof is presented to indicate that not only the chosen plaintext attack but also chosen keyword attack can be resisted in our scheme. Besides, the performance evaluation to be shown indeed depicts its practicability of our scheme for the WBANs.

2. Related Work

In cloud-assisted WBANs, SE [5, 6] can furnish a fundamental solution for data users to issue search queries over the encrypted medical data of a patient generated by WBANs according to his/her interested keywords. Song et al. [5] proposed the first SE scheme, which takes little communication but the computational overhead is proportional to the size of search query. To address this issue, public key encryption with keyword search was proposed [6]. Since then, many different SE schemes were proposed to enrich distinct features such as single keyword search [7, 8], multiple keyword search [9, 10] and fuzzy keyword search [11, 12]. However, the above-mentioned SE schemes with different features do not support data owner to grant the search capability to multiple data users.

To enforce flexible access control over the data, attribute based encryption (ABE) [18–21], including key policy ABE and ciphertext policy ABE, was proposed. Nevertheless, the keyword search functionality is not provided in existing ABE schemes. Motivated by the idea of providing the flexible data search and data share, Zheng et al. [13] introduced two attribute based keyword search (ABKS) schemes, i.e., key policy ABKS (KP-ABKS) and ciphertext policy ABKS (CP-ABKS), by combining the conceptions of SE and ABE together. For the WBANs, CP-ABKS is more suitable than KP-ABKS since data owners are permitted to independently designate access policies themselves to determine who can flexibly search and access the encrypted medical data. Subsequently, several CP-ABKS schemes were also proposed [14–16], whereas these schemes still are inappropriate for the WBANs due to their large computation, communication, and storage costs. To be more specific, in Liang et al.'s scheme [14], the number of pairing and exponentiation operations in both search and decryption phases increases linearly with the complexity of access policy hidden in the ciphertext and the ciphertext size also follows the linear relationship with the complexity of access policy. Although the scheme [15] improves the search efficiency compared to [14], it does not solve the prohibitive computation and communication cost problem like [14, 22]. Besides, this scheme only provides data users with search function but does not support data sharing. In Li et al.'s schemes [16], the computation and storage overhead in both search and decryption phases also follows the linear relationship with the complexity of access policy.

Very recently, although the CP-ABKS [17] that achieves fine-grained access control and search functionality is proposed, its computational and storage overhead is still much more larger. In addition, the reliability of the converted ciphertext returned from the cloud server is not verified. To achieve practicability, feasibility, and verifiability in WBANs, we build a lightweight fine-grained keyword search system based on the scheme [23], which supports flexible access control and single keyword with lightweight and verifiable decryption.

Organization. The rest of organization is introduced as follows. Specifically, Section 3 reviews some basic knowledge including bilinear pairing, hardness assumption, linear secret sharing scheme matrices, etc. Section 4 introduces our system model involving system architecture and threat model. Our proposed system containing system overview and its concrete construction is presented in Section 5. Then, the security analysis and performance analysis are shown in Sections 6 and 7, respectively. Finally, a summary is concluded in the Section 8.

3. Preliminaries

The prime knowledge, including bilinear pairing, hardness assumption, linear secret sharing scheme matrices, and so on, is presented in this part.

3.1. Bilinear Pairing. An algorithm $\mathcal{G}$ based on input a security parameter λ can create a group tuple $(p, \mathbb{G}_0, \mathbb{G}_1, e)$, where $\mathbb{G}_0, \mathbb{G}_1$ of same prime order p denote multiplicative cyclic groups, and a computable bilinear map is represented as $e : \mathbb{G}_0 \times \mathbb{G}_0 \longrightarrow \mathbb{G}_1$ with the properties below: (1) Bilinearity: $e(g_1^s, g_2^t) = e(g_1, g_2)^{st}$ for all $g_1, g_2 \in \mathbb{G}_0$, and $s, t \in \mathscr{Z}_p$. (2) Nondegeneracy: $e(g_1, g_2) \neq 1$.

Denote $\mathbb{U}, \mathbb{V} \in \mathbb{F}_p[\mathbb{X}_1, \ldots, \mathbb{X}_n]^r$ as two r-tuples of n-variate polynomials over $\mathbb{F}_p$, where r, n are integers. That is to say, $\mathbb{U}, \mathbb{V}$ are two lists that contain s multivariate polynomials. Here, we redenote $\mathbb{U} = (u_1, u_2, \ldots, u_r)$, $\mathbb{V} = (v_1, v_2, \ldots, v_r)$ with setting $u_1 = v_1 = 1$. For vector $(\psi_1, \ldots, \psi_n) \in \mathbb{F}_p^n$ and function $h : \mathbb{F}_p \longrightarrow \Omega$, we denote $h(\mathbb{U}(\psi_1, \ldots, \psi_n))$ as $(h(p_1(\psi_1, \ldots, \psi_n))), \ldots, (h(p_r(\psi_1, \ldots, \psi_n))) \in \Omega^s$. We employ the similar notion for r-tuple $\mathbb{V}$. We say that f is based on $(\mathbb{U}, \mathbb{V})$, where $f \in \mathbb{F}_p[\psi_1, \ldots, \psi_n]$. We denote $f \in \langle \mathbb{U}, \mathbb{V} \rangle$ when there is a linear decomposition $f = \sum_{1 \leq i,j \leq r} m_{i,j} \cdot u_i, u_j + \sum_{1 \leq i \leq r} n_i \cdot v_i$, where $m_{i,j}, n_i \in \mathscr{Z}_p$. Then, the definition of (P, Q, f)-GDHE assumption is shown as follows.

Definition 1 ((P, Q, f)-GDHE assumption [23]). Given the tuple $h(\psi_1, \ldots, \psi_n) = (g^{\mathbb{U}(\psi_1, \ldots, \psi_n)}, e(g, g)^{\mathbb{V}(\psi_1, \ldots, \psi_n)})$, the goal is to compute $e(g, g)^{f(\psi_1, \ldots, \psi_n)}$.

Definition 2 ((P, Q, f)-GDDHE assumption [23]). Given the tuple $h(\psi_1, \ldots, \psi_n) = (g^{\mathbb{U}(\psi_1, \ldots, \psi_n)}, e(g, g)^{\mathbb{V}(\psi_1, \ldots, \psi_n)})$, the goal is to decide whether $T = e(g, g)^{f(\psi_1, \ldots, \psi_n)}$.

3.2. Linear Secret Sharing Scheme (LSSS) Matrices. Denote p and $\mathscr{U}$ as a prime order and a universe of attributes. If a collection $\mathbb{A}$ is an access structure on $\mathscr{U}$, then an LSSS matrix $\mathscr{M} \in \mathscr{Z}_p^{l \times n}$ and a function ρ can be found, in which the attribute can be mapped with the function ρ to the rows of matrix $\mathscr{M}$. In this way, an LSSS access policy can be expressed as $(\mathscr{M}, \rho)$. Consider the column vector $\overrightarrow{v} = (t, s_2, \ldots, s_n) \in \mathbb{Z}_p^{*n}$, where t is the shared secret, and $s_2, \ldots, s_n \overset{R}{\leftarrow} \mathscr{Z}_p$. There exist constants $\{\omega_i\}_{i \in I}$ in $\mathscr{Z}_p$ for any shares $\lambda_i = \{\mathscr{M} \cdot \overrightarrow{y}\}_{i \in I}$ of a sharing secret s, $\sum_{i \in I} \omega_i \lambda_i = s$, where $I = \{i \mid i \in [1, l] \vee \rho(i) \in S\}$ and S denotes the authorized set.

3.3. Conversion from a Boolean Formula to an LSSS Matrix. The elaborated working principle of the algorithm in conversion from a Boolean formula to an LSSS matrix can be found in [24]. Here, we briefly introduce its works below: the Boolean formula can be easily converted into an access tree, where AND or OR gates are interior nodes and user attributes acted as the leaf nodes. Here we specify the sharing vector of LSSS matrix as $(1, 0, \ldots, 0)$. As a starting point, the vector (1) is first availed for labelling the root node of the tree and then the levels of the tree are gone down. In this manner, a vector decided by the assigned vector from its parent node is labelled to each node. Besides, an initially global counter variable c to be maintained is set 1. If the parent node is an OR gate with its vector v, then its children are also marked by v. If the parent node is an AND gate with its vector v, 0's at the end are appended after v to make it of length c. Then, vector $v \mid 1$ is distributed to remark one of its children and the vector $(0, \ldots, 0) \mid -1$ is used for labelling another node. It is noteworthy that the summation of these two vectors is $v \mid 0$. The value of c is incremented with 1. Once the whole tree is finished labelling, the rows of LSSS matrix can be built by the vectors. Finally, if the vectors have various lengths, we pad with 0's at the end on the shorter ones to achieve the same length vectors.

3.4. Definition and Security Model of Lightweight Fine-Grained Keyword Search over Encrypted Data. The following algorithms are involved in our lightweight fine-grained keyword search system.

(i) $Setup(1^\lambda, l)$. Inputting the security parameter 1^λ and the attribute universe description, produce the master secret key MSK and the public parameter PP.

(ii) $KeyGen(PP, S, MSK)$. Upon input PP, MSK, and an attribute set S of a user, create the secret key SK for users.

(iii) $Encrypt(PP, \omega, M, \beta)$. Upon input PP, a keyword ω, an access Boolean formula β, and the message M, generate the ciphertext CT with encrypted keyword.

(iv) $Trapdoor(PP, SK, \omega', S)$. On input PP, SK, the picked keyword ω', and S, produce a search token TK for keyword search and a retrieval key RK for message recovery.

(v) $Search(PP, S, TK, CT)$. On input PP, S, TK, and CT, retrieve the intended keyword and then generate the simpler transformed ciphertext CT'.

(vi) $Decrypt(PP, CT', RK, S)$. On input PP, RK, CT', and S, determine the correctness of the decrypted plaintext message M and then recover M if the determined result is true.

Security Model. The security model for our scheme comprises two following probabilistic games between an adversary $\mathscr{A}$ and a challenger $\mathscr{C}$. These two games are used to prove that not only chosen plaintext attack (CPA) but also chosen keyword attack (CKA) can be resisted by our scheme.

CPA-security:

(i) *Init.* The challenge access policy β^* is picked-then-committed to the challenge $\mathscr{C}$ by the adversary $\mathscr{A}$.

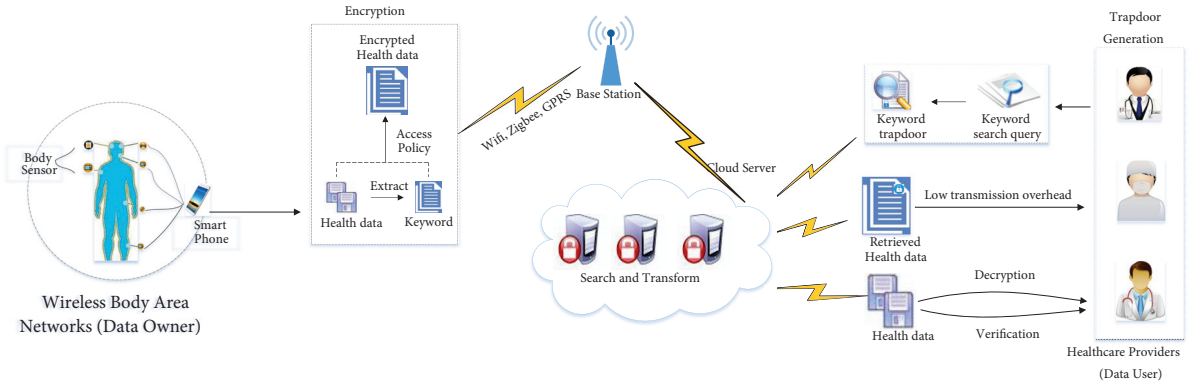


Figure 1: The architecture of our proposed system.

(ii) *Setup.* *Setup* algorithm is done by $\mathscr{C}$ to gain public parameter PP and master secret key MSK. After that, PP is sent to $\mathscr{A}$.

(iii) *Phase* 1&2. *KeyGen* oracle is adaptively queried by $\mathscr{A}$ to obtain secret key by submitting a user attribute S where $S \notin \beta^*$.

(iv) *Challenge.* Two messages M_0, M_1 satisfying $|M_0| = |M_1|$ picked by $\mathscr{A}$ are provided to $\mathscr{C}$. Then, a coin β is first randomly flipped by $\mathscr{C}$ and then the partially generated ciphertext CT_β by running $Encrypt(PK, M_\beta, \beta)$ is transmitted to $\mathscr{A}$.

(v) *Guess.* A guess $\beta' \in \{0, 1\}$ upon β is returned by $\mathscr{A}$.

CKA-Security:

(i) *Init.* The challenge access policy β^* is picked-then-committed to the challenge $\mathscr{C}$ by the adversary $\mathscr{A}$.

(ii) *Setup.* *Setup* algorithm is done by $\mathscr{C}$ to gain public parameter PP and master secret key MSK. After that, PP is sent to $\mathscr{A}$.

(iii) *Phase* 1&2. *Trapdoor* oracle is adaptively queried by $\mathscr{A}$ to gain keyword trapdoor by submitting a user attribute S where $S \notin \beta^*$.

(iv) *Challenge.* Two keywords ω_0, ω_1 meeting $|\omega_0| = |\omega_1|$ picked by $\mathscr{A}$ are provided to $\mathscr{C}$. Then, a coin β is first randomly flipped by $\mathscr{C}$ and then the partially generated ciphertext CT_β by running $Encrypt(PK, \omega_\beta, \beta)$ is transmitted to $\mathscr{A}$.

(v) *Guess.* A guess $\beta' \in \{0, 1\}$ upon β is returned by $\mathscr{A}$.

4. System Model

The system architecture and threat model are presented in the following.

4.1. System Architecture. Figure 1 expressively illustrates the architecture of our proposed scheme, mainly comprising three kinds of entities: the cloud server, the wireless body area networks (WBANs) and the healthcare providers, in which the last two entities are correspondingly regarded as data owners and data users. The function of each entity is described in detail below.

(i) WBANs (Data Owner). Tiny wireless sensors commonly surface-attached on patients' body are comprised in a WBAN. These wireless sensors are employed to monitor the vital physiology parameters such as diabetes, heart rate, and asthma. The collected health data are first aggregated and then delivered to a smart device. After that, keyword to elucidate the information of health data is extracted. Subsequently, the health data with its keyword information are together encrypted into a ciphertext under a self-chosen access policy. Lastly, the encrypted health data are outsourced to the cloud server for remotely sharing data.

(ii) Healthcare provider (Data User). Healthcare providers in our architecture are viewed as data users. Every user owns a list of attributes and red should be allowed to retrieve the encrypted health data relied upon his/her possessed attributes. To search and access the encrypted health data, the data user first creates the keyword trapdoor according to his/her private key and delegates it via wireless channel (e.g., Wifi, Zigbee, and GPRS) to the cloud server for data retrieval. After receiving the returned ciphertex of health data, the data user then decrypts it and verifies the correctness of decryption.

(iii) Cloud Server. The cloud server has almost unlimited storage and computing resources to perform remote storage tasks and respond on data search requests. Besides, in our architecture, the cloud server can also help data user to transform the complex ciphertext of health data into a simple one such that the encrypted health data can be deciphered by the data user in a lightweight way.

Here, note that a fully trusted entity that is called the key generation centre takes charges of authenticating the attributes of users and distributing secret key to data users, which is not provided in our system architecture.

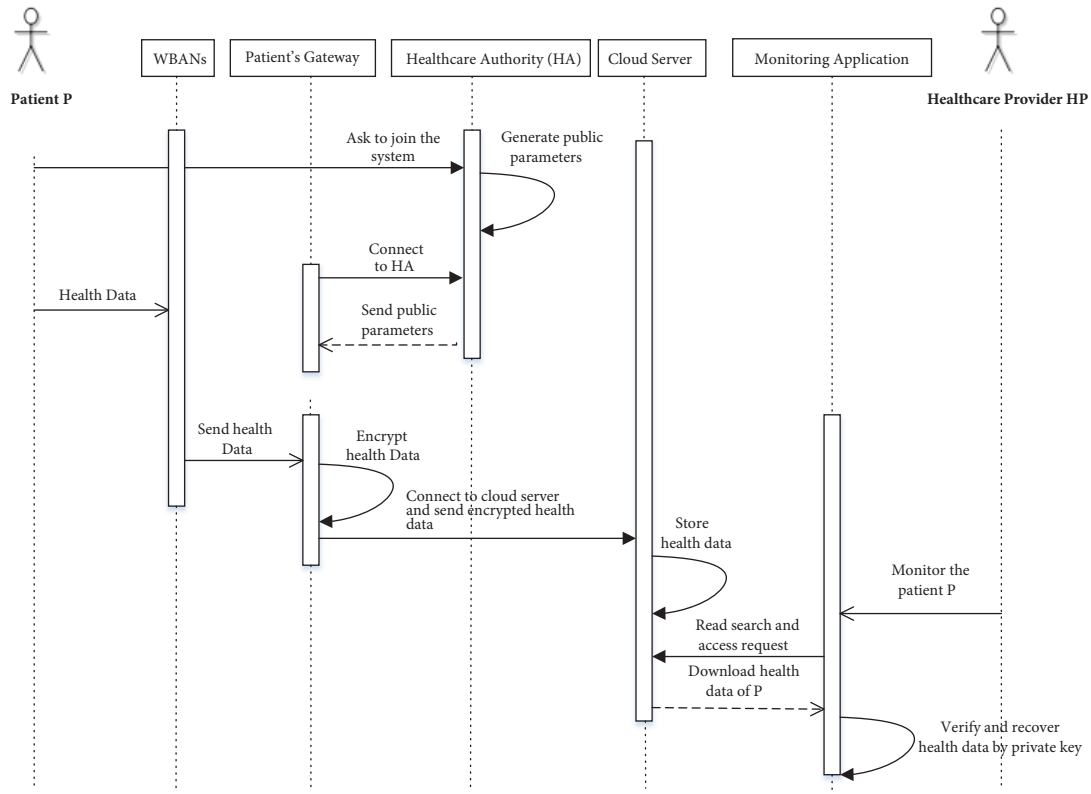


Figure 2: The workflow of our system architecture.

4.2. Threat Model. We suppose that key generation centre is a completely reliable entity and the server is considered as semitrusted and curious. In detail, cloud server is deemed to follow the predefined operations to implement the retrieval task over the encrypted health data but is still curious to gain some sensitive information from the trapdoor or the encrypted health data. Besides, the cloud server may give the incorrectly transformed ciphertext back to the delegated data user for saving its computation resources or bandwidth. In our threat model, all malicious hackers are supposed to own polynomial time bounded computation ability such that they cannot solve the hardness problems.

5. Proposed System

In this section, we first give our system overview and afterward present the detailed construction.

5.1. System Overview. The highlight of our proposed system is to ease the computation overburdens on the user's smart device. The desirable way for data retrieval and data access is to migrate much of the computation-heavy tasks to the cloud server such that data users with the smart device only require to perform certain marginal operations.

The system workflow is in detail described below (shown in Figure 2):

(1) The patient P first asks to join the proposed system. As a response, the healthcare authority (HA) first authenticates the attributes of P and generates the key pair (private key and public key) by implementing *Setup* & *KeyGen* algorithm.

(2) The health data of P are collected and aggregated to a smart device via a WBAN. The P extracts a keyword to describe the health data. Then, both the keyword and health data are created in the form of ciphertext by performing *Encrypt* algorithm. Then P connects via patient's gateway to the cloud server and transmits the encrypted health data with its keyword information. During this process, the access policy picked by the P is also attached to the encrypted health data.

(3) When an authorized health provider (HP) intends to issue data retrieval and data access request, HP first produces a keyword trapdoor by using *Trapdoor* algorithm and delivers it to the cloud server via a monitoring application.

(4) Once gaining the request of search and access, the cloud server uses *Search* algorithm to discover the matched health data and transform the complex ciphertext into a simpler ciphertext, which is then delivered to the HP.

(5) After downloading the simpler ciphertext about health data of the P, HP recovers the health data and checks the correctness of decryption by performing *Decrypt* algorithm.

5.2. Concrete Construction

Setup$(1^\lambda, l)$. Master secret key MSK and public system parameter PP are produced below according to input security parameter 1^λ and attribute universe description. Let $l = |\mathscr{D}|$ denote the maximal number of attributes in the system and $\mathscr{B}=(p, \mathbb{G}_0, \mathbb{G}_1, e(.,.))$ express the bilinear group system. This algorithm first chooses integers $\alpha, a, b, c \in \mathscr{Z}_p$ and one generator g of $\mathbb{G}_0$ in random manners. As well, it selects l group elements $h_1, \ldots, h_l$ from $\mathbb{G}_0$ and two hash functions $H : \{0,1\}^* \longrightarrow \mathscr{Z}_p$, $\mathscr{F} : \{0,1\}^* \longrightarrow \mathscr{K}$. Finally, it publishes $PP = (g, g^a, g^b, g^c, e(g,g)^\alpha, h_1, \ldots, h_l, H, \mathscr{F})$ and keeps $MSK = (a, b, c, \alpha)$ secretly.

KeyGen(PP, S, MSK). On input an attribute set S of a user, the public parameter PP, and the system master key MSK, this algorithm creates the secret key SK for the user as follows: This algorithm first picks $s, t \in \mathscr{Z}_p$ and then computes the secret key for the user as $SK = (d_0 = g^{(ac-\alpha-t)/b}, d_1 = g^\alpha g^{as}, d_2 = g^s, d_3 = g^t, \{f_i = h_i^s\}_{i\in\mathscr{D}})$. Note that user just requires to keep d_1 secret and the rest of other secret key could be published to the public domain [23].

Encrypt(PP, ω, M, β). Upon input the public parameter PP, a keyword ω, an access Boolean formula β, and the message M, this algorithm performs the following procedures: The DNF access policy is described as $\beta = (\beta_1 \vee \cdots \vee \beta_m)$, where β_i is an attribute set, $i = 1, \ldots, m$ and $|m|$ denotes the size of β.

(1) For the certain keyword ω, this algorithm first chooses $\mu, z \in \mathscr{Z}_p$, this algorithm computes $\sigma_1 = g^{a(\mu+z)} g^{b\mu H(\omega)}, \sigma_2 = g^{bz}, \sigma_3 = g^{c\mu}$.

(2) For the plaintext message, it first selects $\chi \in \mathbb{G}_1$ and sets $K_{SE} = \mathscr{F}(\chi)$. After that, $\ell \in \mathscr{Z}_p$ is selected and ℓ-bit 0 string is concatenated after the plaintext message M, which will be exploited to proceed decryption verification. Besides, it computes $C_M = SEnc_{K_{SE}}(M \parallel 0^\ell)$ and $C = \chi \cdot e(g,g)^{\alpha z}, C_0 = g^z$. Then, it compares between l and m. If $l \le |m|$, it computes $C_1 = (g^a \prod_{i\in\beta_i} h_i)^z, \ldots, C_m = (g^a \prod_{i\in\beta_m} h_i)^z$. Else, it reverts to the encryption of the scheme [25]. This algorithm first sets up an LSSS matrix that denotes a map ρ and a Boolean formula β. Next, it picks a vector $\overrightarrow{v} = (z, x_2, \ldots, x_n) \in \mathscr{Z}_p^n$. For $i = 1$ to l, $\lambda_i = \overrightarrow{v}\mathscr{M}_i$ is calculated, where the vector $\mathscr{M}_i$ is equivalent to i-th row of matrix $\mathscr{M}$. Subsequently, it calculates $C_i = g^{a\lambda_i} h_{\rho(i)}^{-z}$, where $i = 1, \ldots, l$.

(3) It finally outputs the ciphertext $CT = (\sigma_1, \sigma_2, \sigma_3, C_0, C_1, \ldots, C_m)$ with a description of β. Or, it returns the ciphertext $CT = (\sigma_1, \sigma_2, \sigma_3, C_M, C_0, C_1, \ldots, C_l)$ with a description of $(\mathscr{M}, \rho)$.

Trapdoor(PP, SK, ω', S). When a user intends to access the data containing the queried keyword, the search token TK can be created as follows: it randomly selects $r \in \mathscr{Z}_p$ and subsequently calculates the search token as $TK = (t_1, t_2, \widehat{d}_0, \widehat{d}_1, \widehat{d}_2, \{\widehat{f}_i\}_{i\in\mathscr{D}})$ and sets retrieval key $RK = r$, where $t_1 = g^{ar} g^{brH(\omega')}, t_2 = g^{cr}, \widehat{d}_0 = d_0^r, \widehat{d}_1 = d_1^r, \widehat{d}_2 = d_2^r, \widehat{d}_3 = d_3^r, \{\widehat{f}_i = f_i^r\}_{i\in\mathscr{D}}$.

Search(PP, S, TD, CT). On input the attribute set S of the user, the search token TK, the public parameter PP, and the ciphertext CT, this algorithm first checks the number elements I of $\mathbb{G}_0$ in CT and whether or not the set of user attributes contents the access policy.

(1) If $I = m + 4$ and the set of user attributes meets the access policy, it computes

$$\begin{aligned}\Theta_1 &= \frac{e\left(C_0, \widehat{d}_1 \prod_{i\in\beta_k} \widehat{f}_i\right)}{e\left(\widehat{d}_2, C_k\right)} = \frac{e\left(g^z, g^{\alpha r}\left(g^a \prod_{i\in\beta_k} h_i\right)^{sr}\right)}{e\left(g^{sr}, \left(g^a \prod_{i\in\beta_k} h_i\right)^z\right)} \\ &= e(g,g)^{\alpha z r}, \\ \Theta_2 &= e\left(\widehat{d}_3, C_0\right) = e(g,g)^{tzr}.\end{aligned} \tag{1}$$

If the attribute set matches the access policy and $I = l + 4$, let $\{\omega_i \in \mathscr{Z}_p\}$ denote a collect of constants satisfying $\sum_{i\in\rho(i)} \omega_i \lambda_i = z$ if the shares $\{\lambda_i\}$ of z are valid. It computes

$$\begin{aligned}\Theta_1 &= e\left(\prod_{i\in\rho(i)} C_i^{-\omega_i}, \widehat{d}_2\right) e\left(C_0, \widehat{d}_1 \prod_{i\in\rho(i)} \widehat{f}_{\rho(i)}^{-\omega_i}\right) \\ &= e\left(\left(\prod_{i\in\rho(i)} g^{a\lambda_i} h_{\rho(i)}^{-z}\right)^{-\omega_i}, g^{sr}\right) \\ &\quad \cdot e\left(g^z, g^{\alpha r} g^{asr} \prod_{i\in\rho(i)} h_{\rho(i)}^{-rs\omega_i}\right) = e(g,g)^{\alpha z r}. \\ \Theta_2 &= e\left(\widehat{d}_3, C_0\right) = e(g,g)^{tzr}.\end{aligned} \tag{2}$$

Otherwise, it aborts and returns $\perp$.

(2) It checks whether $e(\sigma_1, t_2) = e(\sigma_3, t_1) \cdot \Theta_1 \cdot \Theta_2 \cdot e(\sigma_2, \widehat{d}_0)$. If it holds, it returns the outsourced ciphertext $CT' = (\Theta_1, C)$. Otherwise, it also aborts and returns $\perp$.

Decrypt(PP, RK, S). This algorithm executes the following process to recover the encrypted value $\chi = C/\Theta_1^{1/r}$. After that, it computes $K_{SE} = \mathscr{F}(\chi)$ and $M' = SDec_{K_{SE}}(C_M)$. Then, it judges whether a redundancy 0^ℓ is affixed after the decrypted message. If $M \parallel 0^\ell = M'$ holds, M could be gained in the way of truncating ℓ-bit 0 string. Otherwise, it indicates the returned result from the cloud server is incorrect and outputs the symbol $\perp$.

6. Security Analysis

The elaborated security analysis to be presented in this part proves that our scheme is secure. Specifically, not only *CPA*-security but also *CKA*-security can be reached. The following two theorems are utilized to prove its security of the formulated scheme.

Theorem 3. *Our scheme is said to reach the CPA-security under the modified BDHE problem.*

Proof. Provided that the adversary $\mathscr{A}$ can breach our scheme, then there exists another algorithm $\mathscr{C}$ that could be built to address the modified BDHE problem by exploiting the interaction chance with $\mathscr{A}$. Given the modified BDHE-assumption instance $(g, g^{\rho}, g^{\tau}, \ldots, g^{\tau^{q}}, g^{\tau^{q+2}}, \ldots, g^{\tau^{2q}}, g^{\rho(\tau+\tau\eta)}, g^{\tau\eta}, g^{\tau^{2}\eta}, \ldots, g^{\tau^{q}\eta}, g^{\tau^{q+2}\eta}, \ldots, g^{\tau^{2q}\eta})$. $\mathscr{C}$ avails of $\mathscr{A}$ and simulates the process of the game to determine if $\mathscr{Z} = e(g,g)^{\tau^{q+1}\rho}$, or $\mathscr{Z}$ is an element randomly chosen from $\mathbb{G}_1$. □

Setup. A challenge access policy $\beta^* = \beta_1^* \vee \cdots \vee \beta_m^*$ is picked by $\mathscr{A}$ and sent to $\mathscr{C}$. Here suppose that $|\beta^*|$ denotes the size of the challenge access policy β^*, where β_i^* are disjoint sets. Then $\mathscr{C}$ creates *PK* by considering the cases below.

(i) Case 1. If $m > |\beta^*|$, the process of the public system parameter generation in our scheme is almost the same as that in the scheme [25]. Here we refer readers to the proof in [25]. It is worth noting that the modified BDHE assumption is an extension of the BDHE assumption.

(ii) Case 2. If $m \le |\beta^*|$, the challenger $\mathscr{C}$ first builds LSSS matrix $(\mathscr{M}^*_{l^* \times n^*}, \rho^*)$. Next, $\mathscr{C}$ picks $\tau' \in \mathscr{Z}_p$ and sets $e(g,g)^{\alpha} = e(g^{\tau}, g^{\tau^{q}}) e(g,g)^{\tau'} = e(g,g)^{\tau'+\tau^{q+1}}$, $g^{a} = g^{\tau}$. Next, $\mathscr{C}$ discovers disjoint sets of rows of $\mathscr{M}^*$: $J_1, \ldots, J_m$, where $\{\rho(i), i \in J_j\} = \beta_j^*$. β_j^* is described as $(\wedge\rho(i))_{i\in J_1} \vee (\wedge\rho(i))_{i\in J_2} \vee \cdots \vee (\wedge\rho(i))_{i\in J_m}$. Then, the vector $\overrightarrow{y} = (\tau, \tau\eta, \ldots, \tau^{n^*-1}\eta)$ is implicitly defined by $\mathscr{C}$ such that $\overrightarrow{\lambda} = \sum_{k\in[1,n^*]} \mathscr{M}^* \cdot \overrightarrow{y}$. Specifically, $\overrightarrow{\lambda}_j = \sum_{k\in[1,n^*]} \mathscr{M}^*_{j,i} t a^{i-1}$ for $j = 1, \ldots, l^*$. In addition, $\mathscr{C}$ also discovers set $\{\omega_i\}_{i\in[1,l^*]}$ satisfying $\sum \omega_i \lambda_i = \tau$. For each h_j, if $j \in [1,l]$, where there exists an index $i \in [1,l^*]$, then $\mathscr{C}$ picks $t_j \in \mathscr{Z}_p$ and computes $h_j = g^{t_i} g^{\omega_i \sum_{k\in[1,n^*]} \mathscr{M}^*_{j,i} t a^{i}} = g^{t_j} g^{\tau\omega_i\lambda_i}$. Otherwise, $\mathscr{C}$ picks $t_j \in \mathscr{Z}_p$ and computes $h_j = g^{t_j}$. Finally, $PK = (g, g^{a}, e(g,g)^{\alpha}, h_1, \ldots, h_l)$ is published by $\mathscr{C}$.

Phase 1&2. The challenger $\mathscr{C}$ generates the secret key as follows: $\mathscr{A}$ first issues the set of indices of attributes $\mathcal{S} \in [1,l]$ to $\mathscr{C}$; here $\mathcal{S} \not\models \mathscr{M}^*$ (this means that the set of indices of attributes does not match the matrix $\mathscr{M}^*$). A vector $\overrightarrow{x} = (x_1, x_2, \ldots, x_{n^*})$, satisfying $x_1 = -1$ and the inner product $\langle \overrightarrow{x}, \mathscr{M}_i^* \rangle = 0$, is first picked by $\mathscr{C}$. Then, $\mathscr{C}$ picks $\theta \in \mathscr{Z}_p$ and computes

$$
\begin{aligned}
d_1 &= g^{\tau'} g^{\tau\theta} \prod_{i=2,\ldots,n^*} \left(g^{\tau^{q+2-i}}\right)^{x_i} \\
&= g^{\tau'} \left(g^{\tau}\right)^{\theta+\tau^{q}x_1+\tau^{q-1}x_2+\cdots+\tau^{q-n^*+1}x_{n^*}-\tau^{q}x_1} \\
&= g^{\tau'+\tau^{q+1}} \left(g^{\tau}\right)^{\theta+\tau^{q+1}x_1+\tau^{q-2}x_2+\cdots+\tau^{q-n^*}x_{n^*}} = g^{\alpha} g^{as}, \\
d_2 &= g^{\theta} \prod_{i=1,\ldots,n^*} \left(g^{\tau^{q+1-i}}\right)^{x_i} = g^{\theta+\tau^{q}x_1+\tau^{q-1}x_2+\cdots+\tau^{q-n^*+1}x_{n^*}} \\
&= g^{s},
\end{aligned}
\tag{3}
$$

where $s = \theta + \tau^{q}x_1 + \tau^{q-1}x_2 + \cdots + \tau^{q-n^*+1}x_{n^*}$.

For $j \in \mathcal{S}$ if there exists no $i \in [1,l^*]$ matching $\rho^*(i) = j$, $\mathscr{C}$ computes $f_j = (g^{s})^{t_j} = (g^{t_j})^{s} = h_j^{s}$. For $j \in \mathcal{S}$ such that there exists an index $i \in [1,l^*]$ matching $\rho^*(i) = j$; $\mathscr{C}$ computes $f_j = (g^{s})^{t_j} g^{(\theta+\tau^{q}x_1+\tau^{q-1}x_2+\cdots+\tau^{q-n^*+1}x_{n^*})\sum_{k\in[1,n^*]} \mathscr{M}^*_{j,i} t a^{i-1}} = (g^{t_j})^{s} = h_j^{s}$. Note that $\langle \overrightarrow{x}, \mathscr{M}_i^* \rangle = 0$. Thus, the partial secret key can be created as (d_1, d_2, f_j) .

Challenge. Two plaintext messages M_0^* and M_1^* with equal length are picked-then-delivered to $\mathscr{C}$. Then, $\mathscr{C}$ selects $\beta \in \{0,1\}$ and subsequently computes as follows:

$$
\begin{aligned}
C &= M_{\beta} \cdot \mathscr{Z} \cdot e\left(g^{\rho}, g^{\tau'}\right) = M_{\beta} \cdot \mathscr{Z} \cdot e\left(g^{z}, g^{\tau'}\right), \\
C_0 &= g^{\rho} = g^{z}, \\
C_1 &= g^{\rho(\tau+\tau\eta)} g^{\sum_{i\in J_1} \rho t_{\rho(i)}} = \left(g^{\tau} \cdot \prod_{i\in J_1} g^{t_{\rho(i)}} g^{\tau\omega_i\lambda_i}\right)^{\rho}, \\
&= \left(g^{\tau} \prod_{i\in J_1} h_{\rho(i)}\right)^{\rho} \\
&= \left(g^{\tau} \prod_{i\in \beta_1} h_i\right)^{\rho} \\
&= \left(g^{\tau} \prod_{i\in \beta_1} h_i\right)^{z}, \\
&\vdots \\
C_m &= g^{\rho(\tau+\tau\eta)} g^{\sum_{i\in J_m} \rho t_{\rho(i)}} \\
&= \left(g^{\tau} \cdot \prod_{i\in J_m} g^{t_{\rho(i)}} g^{\tau\omega_i\lambda_i}\right)^{\rho}, \\
&= \left(g^{\tau} \prod_{i\in J_m} h_{\rho(i)}\right)^{\rho} \\
&= \left(g^{\tau} \prod_{i\in \beta_m} h_i\right)^{\rho}, \\
&= \left(g^{\tau} \prod_{i\in \beta_m} h_i\right)^{z}.
\end{aligned}
\tag{4}
$$

Note that here we use M_{β} instead of the selected symmetry key to simulate the whole game.

Table 1: Function comparison with other schemes.

Scheme	Fine-Grained	Keyword Search	Data Sharing	Verifiable Decryption
[13]	√	√	×	×
[14]	√	√	√	×
[15]	√	√	×	×
[16]	√	√	√	×
[17]	√	√	√	×
Ours	√	√	√	√

Guess. A guess with $\beta' \in \{0,1\}$ upon β is responded by $\mathcal{A}$, then $\mathcal{C}$ gives 1 to guess $\mathcal{Z} = e(g,g)^{\tau^{q+1}\rho} = e(g,g)^{\tau^{q+1}z}$ if holding $\beta = \beta'$. Otherwise, $\mathcal{C}$ guesses that $\mathcal{Z}$ is an element randomly picked from $\mathbb{G}_1$.

Theorem 4. *The proposed scheme is said to achieve the CKA-security in the general bilinear group model, where H is regarded as a random oracle.*

Proof. In this game, the adversary will intend to distinguish $g^{a(\mu+z)}g^{b\mu H(\omega)}$ from $g^{a(\mu+z)}g^{b\mu H(\omega')}$. Given $\varrho \in \mathcal{Z}_p$, the probability of distinguishing $g^{a(\mu+z)}g^{b\mu H(\omega)}$ from g^{ϱ} is the same as that of differentiating $g^{a(\mu+z)}g^{b\mu H(\omega')}$ from g^{ϱ}. If $\mathcal{A}$ has an advantage $\varrho/2$ in breaching this game, then $\mathcal{A}$ has the same advantage in differentiating $g^{a(\mu+z)}g^{b\mu H(\omega)}$ from g^{ϱ}. In this way, we can modify the above game as that $\mathcal{A}$ can distinguish $g^{a(\mu+z)}$ from g^{ϱ}. The elaborated proof of the modified game is explained below.

(i) *Setup*. The challenger $\mathcal{C}$ randomly picks $a,b,c \in \mathcal{Z}_p$, transmits the produced tuple (e,g,g^a,g^b,g^c) to $\mathcal{A}$. Subsequently, $\mathcal{A}$ chooses an access policy β^* and sends it to $\mathcal{C}$. Lastly, $\mathcal{C}$ proceeds the following simulation. Concretely, if $\mathcal{A}$ submits the attribute i that has not been issued before, $\mathcal{C}$ picks $\theta_i \in \mathcal{Z}_p$, then added (i,θ_i,h_i) to the list $\mathcal{O}_H$ and returns $h_i = g^{\theta_i}$. Otherwise, $\mathcal{C}$ directly returns $h_i = g^{\theta_i}$ by picking out θ_i from $\mathcal{O}_H$.

(ii) *Phase* 1&2. $\mathcal{A}$ will query $\mathcal{O}_{SK}$ and $\mathcal{O}_{TK}$ to gain secret key SK and search token TK below.

(a) $\mathcal{O}_{SK}$: After receiving the attribute set S^* from $\mathcal{A}$, $\mathcal{C}$ first chooses $\alpha, t^*, s^* \in \mathcal{Z}_p$ and computes $d_0 = g^{(ac-\alpha-t^*)/b}$, $d_1 = g^{\alpha}(g^a)^{s^*}$, $d_2 = g^{s^*}$, $d_3 = g^{t^*}$, $f_i = g^{\theta_i s^*}$. Then, $\mathcal{C}$ returns the secret key $SK = (d_0, d_1, d_2, d_3, \{f_i\}_{i\in\mathcal{S}^*})$.

(b) $\mathcal{O}_{TK}$: $\mathcal{A}$ queries the oracle $\mathcal{O}_{SK}$ to get $SK = (d_0, d_1, d_2, d_3, \{f_i\}_{i\in\mathcal{S}^*})$. Then, $\mathcal{C}$ chooses r^* and produces the search token $TK = (t_1, t_2, \hat{d}_0, \hat{d}_1, \hat{d}_2, \{\hat{f}_i\}_{i\in\mathcal{S}^*})$, where $t_1 = g^{ar^*}g^{br^*H(\omega')}$, $t_2 = g^{cr^*}$, $\hat{d}_0 = d_0^{r^*}$, $\hat{d}_1 = d_1^{r^*}$, $\hat{d}_2 = d_2^{r^*}$, $\hat{d}_3 = d_3^{r^*}$, $\{\hat{f}_i = f_i^{r^*}\}_{i\in\mathcal{S}^*}$ and also embeds the keyword ω' into the keyword list L.

(iii) *Challenge*. On giving two challenge keywords $\hat{\omega}, \tilde{\omega}$ with equal length, where $\hat{\omega}, \tilde{\omega} \notin L$, $\mathcal{C}$ first chooses $\mu, z \in \mathcal{Z}_p$. Next, $\mathcal{C}$ picks a random bit $\tau \in \{0,1\}$. If $\tau = 0$, then $\mathcal{C}$ computes and returns $\sigma_1 = g^{\varrho}$, $\sigma_2 = g^{bz}$, $\sigma_3 = g^{c\mu}$, $C_0 = g^z$ and $C_i = (g^a\prod_{i\in\beta^*}g^{\rho_i})^z$. Otherwise, $\mathcal{C}$ sets and returns $\sigma_1 = g^{a(\mu+z)}$, $\sigma_2 = g^{bz}$, $\sigma_3 = g^{c\mu}$, $C_0 = g^z$ and $C_i = (g^a\prod_{i\in\beta^*}g^{\theta_i})^z$. Finally, $\mathcal{C}$ sends the challenge ciphertext to $\mathcal{A}$.

We can gain that if $\mathcal{A}$ can build $e(g,g)^{\xi a(\mu+z)}$ for some g^{ξ} which is comprised by the outputs in Phase 1&2, then $\mathcal{A}$ can differentiate g^{ϱ} from $g^{a(\mu+z)}$. Here, we still require to demonstrate that $e(g,g)^{\xi a(\mu+z)}$ for some g^{ξ} could be built by $\mathcal{A}$ with a negligible advantage. That is to say, $\mathcal{A}$ cannot breach the CKA game with a nonnegligible advantage. □

In the general group, given the two groups $\mathbb{G}_0 = \{\psi_0(\epsilon) \mid \epsilon \in \mathcal{Z}_p\}$ and $\mathbb{G}_1 = \{\psi_1(\epsilon) \mid \epsilon \in \mathcal{Z}_p\}$, where ψ_0 and ψ_1 are two random injective maps from $\mathcal{Z}_p$ into a set of p^3 elements, $\mathcal{A}$ can guess the image of ψ_0 and ψ_1 with a negligible advantage. So let us consider how to construct $e(g,g)^{\xi a(\mu+z)}$ for $\xi \in \mathcal{Z}_p$. Since only the term $c\mu$ contains the element μ, so in order to build the $e(g,g)^{\xi a(\mu+z)}$, ξ must include the factor c. In other words, $\xi = c\xi'$ and $\mathcal{A}$ desires to build $e(g,g)^{\xi' ac(\mu+z)}$. Here, $\mathcal{A}$ can use $\sigma_2 = g^{bz}$ and $d_0 = g^{(ac-\alpha-t^*)/b}$ to get $e(g,g)^{(ac-\alpha-t^*)z}$. Although $\mathcal{A}$ can get $e(g,g)^{(ac-\alpha-t^*)z}$, $\mathcal{A}$ still needs to cancel $e(g,g)^{(\alpha+t^*)z}$ by using $d_1 = g^{\alpha}(g^a)^{s^*}$, $d_2 = g^{s^*}$, $d_3 = g^{t^*}$, and $f_i = g^{\theta_i s^*}$. However, $\mathcal{A}$ cannot build these items since $e(g,g)^{(\alpha+t^*)z}$ can only be built on the condition that the attributes content the access policy β^*. Therefore, we cannot derive that $\mathcal{A}$ can breach the CKA game.

7. Performance Analysis

With respect to function, storage cost, and computation overhead, this part presents comparisons among other existing attribute based keyword search schemes and our proposed scheme.

7.1. Qualitative Analysis. Table 1 shows the function comparison with other schemes [13–17]. From the Table 1, we can learn that all schemes provide fine-grained keyword search. Data sharing is achieved in our scheme and [14, 16, 17]. Verifiable decryption among [14, 16, 17] and ours is only dealt with in our scheme. In summary, our scheme is only one that can achieve all functionalities including fine-grained keyword search and data sharing and verifiable decryption.

Table 2 presents performance comparisons with other schemes with regard to the storage and computation

Table 2: Storage and computation overhead comparison with other schemes.

Scheme	|PP|	|SK|	|CT|	|TK|	Enc	Search	Dec
[13]	$3\lvert\mathbb{G}_0\rvert$	$2S\lvert\mathbb{G}_0\rvert$	$(l+3)\lvert\mathbb{G}_0\rvert$	$(2S+2)\lvert\mathbb{G}_0\rvert$	$(S+4)t_{e_1}$	$(2S+2)t_p$	$\perp$
[14]	$(2\lvert U\rvert+10)\lvert\mathbb{G}_0\rvert+3\lvert\mathbb{G}_1\rvert$	$3S\lvert\mathbb{G}_0\rvert$	$(l+3)\lvert\mathbb{G}_0\rvert+2\lvert\mathbb{G}_1\rvert$	$3S\lvert\mathbb{G}_0\rvert$	$2t_p+2t_{e_2}+(l+5)t_{e_1}$	$2t_p+2lt_{e_1}$	$4t_p+t_{e_2}+(3l+4)t_{e_1}$
[15]	$(3\lvert U\rvert+1)\lvert\mathbb{G}_0\rvert+\lvert\mathbb{G}_1\rvert$	$(2S+1)\lvert\mathbb{G}_0\rvert+\lvert\mathscr{Z}_p\rvert$	$(l+2)\lvert\mathbb{G}_0\rvert$	$(2S+2)\lvert\mathbb{G}_0\rvert$	$(2S+2)t_{e_1}$	$(S+1)t_p+t_{e_2}$	$\perp$
[16]	$(\lvert U\rvert+2)\lvert\mathbb{G}_0\rvert$	$2S\lvert\mathbb{G}_0\rvert$	$(l+1)\lvert\mathbb{G}_0\rvert+\lvert\mathbb{G}_1\rvert$	$(2S+1)\lvert\mathbb{G}_0\rvert$	$(S+1)t_{e_1}+t_{e_2}$	$(S+2)t_p$	$(2l+2)t_p$
[17]	$(\lvert U\rvert+4)\lvert\mathbb{G}_0\rvert$	$(S+1)\lvert\mathbb{G}_0\rvert+\lvert\mathscr{Z}_p\rvert$	$(2l+4)\lvert\mathbb{G}_0\rvert+\lvert\mathbb{G}_1\rvert$	$(2S+3)\lvert\mathbb{G}_0\rvert$	$(S+1)t_{e_1}+t_{e_2}$	$(2S+1)t_p+St_{e_1}$	$(l+3)t_p$
Ours	$(\lvert U\rvert+3)\lvert\mathbb{G}_0\rvert+\lvert\mathbb{G}_1\rvert$	$\lvert\mathbb{G}_0\rvert$	$(l+4)\lvert\mathbb{G}_0\rvert+\lvert\mathbb{G}_1\rvert$	$(S+6)\lvert\mathbb{G}_0\rvert$	$(2S+5)t_{e_1}+t_{e_2}$	$3t_p+2St_{e_1}$	t_{e_1}

overhead. In this table, |PP|, |SK|, |CT| and |TK| denote the sizes of public parameter, secret key, ciphertext and trapdoor. Let $|S|$ and $|U|$ in turn represent the sizes of attribute set and universe attribute set. Denote l as the number of rows in the matrix. In addition, an element bit length in corresponding group $\mathbb{G}_0$, $\mathbb{G}_1$, and $\mathscr{Z}_p$ is denoted as $|\mathbb{G}_0|$, $|\mathbb{G}_1|$, and $|\mathscr{Z}_p|$. Let t_{e_1}, t_{e_2} stand for the time consuming in modular exponentiations on group $\mathbb{G}_0$, $\mathbb{G}_1$, and t_p be time cost in a bilinear pairing, respectively.

Table 2 shows that our proposed scheme has optimal sizes no matter what the sizes are secret key size, ciphertext size, and even trapdoor size. Besides, it has higher computation efficiency on encryption, search, and decryption algorithm. The detailed analyzing is presented as follows: It is easy to see that our scheme consists of an element size on group $\mathbb{G}_1$ and $|U| + 3$ element sizes on group $\mathbb{G}_0$. Obviously, it is much more smaller than that in [14, 15, 17]. For the secret key size, our scheme only has an element in group $\mathbb{G}_0$, which is the smallest compared to the other schemes. For user's resource-limited mobile device, smaller secret key size commonly implies smaller storage cost. Our scheme also has a smaller size in both the ciphertext size and trapdoor size. For the computation overhead for encryption, search, and decryption, our scheme could use $(2S + 5)$ exponentiation operations on group $\mathbb{G}_0$ and an exponentiation on group $\mathbb{G}_2$ for encryption. which has a little higher than that in other schemes. For the computation overhead of search, our scheme has three bilinear pairing operations and $2S$ exponentiation operations on group $\mathbb{G}_0$, which reaches the best efficiency compared to other schemes, since the time consuming of other schemes follows linear relationship with the number of bilinear pairing operations whereas it in ours is growing linearly with the amount of exponentiation operations on group $\mathbb{G}_0$. For the computation overhead on decryption, only our scheme can achieve constant computation while other schemes cannot achieve it. This signifies that our scheme is still stable even though the number of involved attributes are too lager, which makes our scheme practical for the mobile device.

7.2. Experimental Result. The type A elliptic curve of 160-bit group order in pbc library [26], as the best curve to produce the fast bilinear pairing, is picked for experimental test, which is commonly deemed to have 80-bit security level. The curve expression E is denoted as $y^2 = x^3 + x$ over $\mathbb{F}_q$ finite field. Both group $\mathbb{G}_0$ and $\mathbb{G}_1$ with same prime order p are subgroup of $E(\mathbb{F}_q)$. Then, we can get $|\mathscr{Z}_p| = 20$ bytes, $|\mathbb{G}_0| = |\mathbb{G}_1| = 128$ bytes. In our experiment test, data owners equipped with personal computers (PC) are commonly considered to have abundant resources to perform encryption to produce the data ciphertext, which will be remotely shared on the cloud server, which has powerful computing capabilities to perform the search and outsourcing decryption tasks. Due to the capacity limited mobile devices, end users (data users) require to delegate the computation-intensive operation of search and decryption to cloud server for releasing their burdens such that few lightweight operations are only done by themselves. Here, we proceed our experimental simulation according to the data from Yang et al.'s scheme [27]. More concretely, the computation times on PC for a bilinear pairing operation, an exponentiation on group $\mathbb{G}_0$, and an exponentiation on group $\mathbb{G}_1$ are 18.02ms, 9.17ms, and 2.78ms, respectively. The computation times on smart phone for those are 195.11ms, 90.12ms, and 33.40ms. Note that PC and smart phone act as cloud server and data user, respectively. Here, the schemes [14, 16, 17] achieving keyword search and data access simultaneously are compared to our scheme in terms of the storage and computation overhead in Figure 3. In detail, the secret key size comparison, ciphertext size comparison, and trapdoor size comparison are given in Figures 3(a), 3(b), and 3(c), respectively. The encryption time comparison, search time comparison, and decryption time comparison are given, respectively, in Figures 3(d), 3(e), and 3(f). It is explicit to see that our scheme has a satisfactory performance in smaller secret key size, trapdoor size, and decryption cost.

In summary, our proposed scheme is almost superior to the existing related schemes since it has an extremely lightweight data access, which proves that our scheme is more feasible if being applied in IoT applications.

8. Conclusion

In this paper, a lightweight search with fine-granularity over encrypted data in WBANs is proposed. With our proposed scheme, the healthcare provider can achieve fast keyword search and lightweight verifiable decryption in the manner of fine-granularity. In addition, this paper also formally defines the security of the proposed scheme and proves its security in the random oracle. Finally, the qualitative analysis and practical simulations to be presented in this paper confirm that our proposed scheme is indeed of high efficiency and good feasibility for WBANs. Constructing a scheme that achieves conjunctive keyword search, attribute update, or the verifiability for both decryption and search would be our main future focus.

Data Availability

The data used to support the findings of this study are included within the article. In detail, please refer to the detailed descriptions in experimental result part.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by NSFC (no. 61472064).

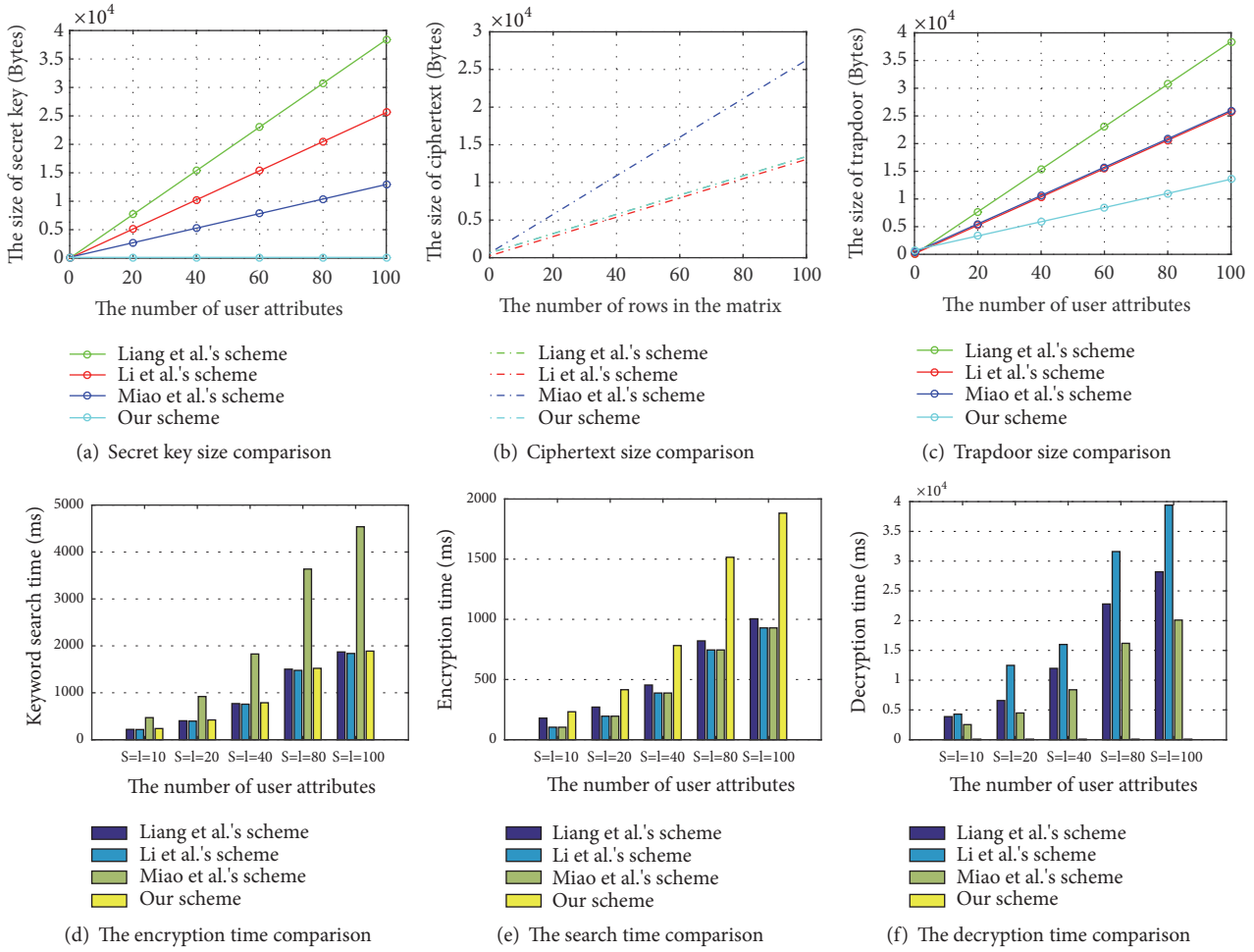


Figure 3: Storage and computation overhead comparison.

References

[1] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[2] M. Li, W. J. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications Magazine*, vol. 17, no. 1, pp. 51–58, 2010.

[3] D. Chen, N. Zhang, R. Lu, N. Cheng, K. Zhang, and Z. Qin, "Channel Precoding Based Message Authentication in Wireless Networks: Challenges and Solutions," *IEEE Network*, pp. 1–7.

[4] Q. Wang, D. Chen, and N. Zhang, "LACS: A Lightweight Label-Based Access Control Scheme in IoT-Based 5G Caching Context," *IEEE Access*, 4027 pages, 2017.

[5] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P '00)*, pp. 44–55, IEEE, Berkeley, Calif, USA, May 2000.

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology—EUROCRYPT 2004*, vol. 3027 of *Lecture Notes in Computer Science*, pp. 506–522, Springer, Berlin, Germany, 2004.

[7] H. Li, D. Liu, Y. Dai, T. H. Luan, and S. Yu, "Personalized search over encrypted data with efficient and secure updates in mobile clouds," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 1, pp. 97–109, 2018.

[8] Y. Miao, J. Ma, and Z. Liu, "Revocable and anonymous searchable encryption in multi-user setting," *Concurrency Computation*, vol. 28, no. 4, pp. 1204–1218, 2016.

[9] Y. Yang and M. Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 746–759, 2016.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222–233, 2014.

[11] C. Liu, L. Zhu, L. Li, and Y. Tan, "Fuzzy keyword search on encrypted cloud storage data with small index," in *Proceedings of the 2011 IEEE International Conference on Cloud Computing and Intelligence Systems, CCIS2011*, pp. 269–273, China, September 2011.

[12] J. Wang, H. Ma, Q. Tang et al., "Efficient verifiable fuzzy keyword search over encrypted data in cloud computing," *Computer Science and Information Systems*, vol. 10, no. 2, pp. 667–684, 2013.

[13] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: privacy-preserving outsourcing computation of feature extractions over encrypted image data," *IEEE Transactions on Image Processing*, vol. 25, no. 7, pp. 3411–3425, 2016.

[14] K. Liang and W. Susilo, "Searchable Attribute-Based Mechanism With Efficient Data Sharing for Secure Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1981–1992, 2015.

[15] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting Your Right: Verifiable Attribute-Based Keyword Search with Fine-Grained Owner-Enforced Search Authorization in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 4, pp. 1187–1198, 2016.

[16] J. G. Li, X. N. Lin, Y. C. Zhang, and J. G. Han, "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 715–725, 2017.

[17] Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, "Lightweight Fine-Grained Search over Encrypted Data in Fog Computing," *IEEE Transactions on Services Computing*, 2018.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, November 2006.

[19] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, May 2007.

[20] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in *Public Key Cryptography (PKC '11)*, pp. 53–70, Springer, Berlin, Germany, 2011.

[21] X. Fu, X. Nie, T. Wu, and F. Li, "Large universe attribute based access control with efficient decryption in cloud storage system," *The Journal of Systems and Software*, vol. 135, pp. 157–164, 2018.

[22] Q. Wang, D. Chen, N. Zhang, Z. Ding, and Z. Qin, "PCP: A Privacy-Preserving Content-Based Publish-Subscribe Scheme with Differential Privacy in Fog Computing," *IEEE Access*, vol. 5, pp. 17962–17974, 2017.

[23] Q. M. Malluhi, A. Shikfa, and V. C. Trinh, "A ciphertext-policy attribute-based encryption scheme with optimized ciphertext size and fast decryption," in *Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security (ASIA CCS '17)*, pp. 230–240, New York, NY, USA, April 2017.

[24] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proceedings of the Annual international conference on the theory and applications of cryptographic techniques*, pp. 568–588, Springer, Berlin, Heidelberg, 2011.

[25] S. Hohenberger and B. Waters, "Attribute-Based Encryption with Fast Decryption," in *Public-Key Cryptography – PKC 2013*, vol. 7778 of *Lecture Notes in Computer Science*, pp. 162–179, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[26] B. Lynn, Pbc library, 2006, http://crypto.stanford.edu/pbc.

[27] Y. Yang, X. Liu, R. H. Deng, and Y. Li, "Lightweight Sharable and Traceable Secure Mobile Health System," *IEEE Transactions on Dependable and Secure Computing*, 2017.

Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 4870656, 10 pages
https://doi.org/10.1155/2019/4870656

Research Article

Machine Learning Based Antenna Design for Physical Layer Security in Ambient Backscatter Communications

Tao Hong,[1] **Cong Liu**,[1] **and Michel Kadoch**[2]

[1]*School of Electronics and Information Engineering, Beihang University, China*
[2]*Department of Electrical Engineering, École de Technologie Supérieure, University of Quebec, Canada*

Correspondence should be addressed to Tao Hong; hongtao@buaa.edu.cn

Received 4 October 2018; Accepted 4 December 2018; Published 1 January 2019

Guest Editor: Feng Ye

Ambient backscatter employs existing radio frequency (RF) signals in the environment to support sustainable and independent communications, thereby providing a new set of applications that promote the Internet of Things (IoT). However, nondirectional forms of communication are prone to information leakage. In order to ensure the security of the IoT communication system, in this paper, we propose a machine learning based antenna design scheme, which achieves directional communication from the relay tag to the receiving reader by combining patch antenna with log-periodic dual-dipole antenna (LPDA). A multiobjective genetic algorithm optimizes the antenna side lobe, gain, standing wave ratio, and return loss, with a goal of limiting the number of large side lobes and reduce the side lobe level (SLL). The simulation results demonstrate that our proposed antenna design is well suited for practical applications in physical layer security communication, where signal-to-noise ratio of the wiretap channel is reduced, communication quality of the main channel is ensured, and information leakage is prevented.

1. Introduction

The Internet of Things (IoT) is a vital component of the fifth generation (5G) mobile communications, interconnecting a large number of devices. However, in traditional backscatter communication systems, radio frequency (RF) power is provided by the reader, and the limited power supply limits the widespread use of IoT.

In 2013, the proposed ambient backscatter communication technology solved some of the above shortcomings [1]. Unlike traditional backscatter communication (e.g., for passive sensors and RF identification (RFID) tags), ambient backscatter does not require specific devices to provide energy but instead utilizes RF signals in the environment as both energy resources and signal resources for reflection [2]. As a result, ambient backscatter provides sustainable and independent communications, and the maintenance and implementation costs of the system can be greatly reduced [3, 4]. Because the ambient configuration does not require additional spectrum resources to operate, we chose the 4G, 5G, and Wireless-Fidelity (Wi-Fi) signals with frequencies in the range of 2 GHz - 4 GHz as the ambient resources.

However, several challenges remain. The broadcast characteristics of wireless signals make it easy for some illegal eavesdroppers to obtain information content, and signals of the same frequency are superimposed at the receiver to cause interference, which brings many difficulties to signal detection [5].

Traditional security techniques, which encrypt information with high computationally complex codec algorithms [6], have gradually failed with the rapid increase in the computational power. The fundamental principle behind physical layer security is to exploit the inherent randomness of noise and communication channels to limit the amount of information that can be extracted at the "bit" level by an unauthorized receiver [7]. Therefore, information-theoretic security is considered to be a key technology to ensure the security of wireless communications.

A lot of research has been done on physical layer security. A cooperative relay scheme was investigated in [8]; however it is only applicable to multiantenna and multirelay systems. Artificial noise- (AN-) based methods are also inappropriate because of their higher energy expenditure and increased cochannel interference with any adjacent user [9].

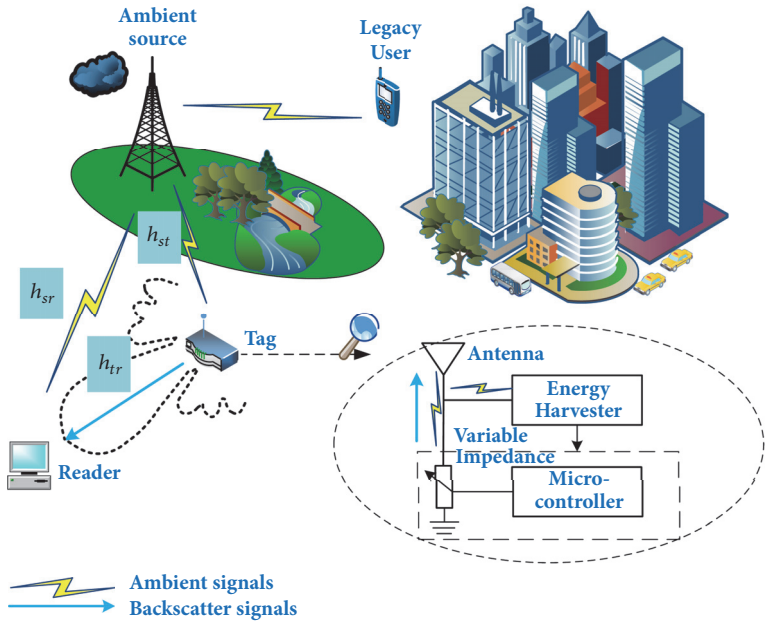


Figure 1: Ambient backscatter system.

Comparisons have shown that the method most suited for IoT sensing applications is beamforming, which allows the signal to propagate in a specified direction [10]. Through beamforming technology, the signal-to-noise ratio (SNR) is increased at the legitimate reader whereas it is reduced at the illegal eavesdropper, thereby enhancing the security performance of the system.

In order to achieve similar beamforming functions in a sensor network, we focused our research on the antenna design of the relay tag. Existing relay antennas have problems such as very large size, poor directivity, and small transmission gain [11]. We designed a dual-antenna system consisting of a patch antenna array and a printed log-periodic dual-dipole antenna (LPDA) with the advantages of orientation and high gain. At the same time, it has a fairly wide operating frequency band, which can effectively utilize various types of signals in the environment. Moreover, the small side lobes reduce the SNR received by eavesdroppers from other directions, ensuring the security of communication. In practical applications, the patch antenna array receives RF signals from all directions and then transmits them through the LPDA in a specified direction.

Traditional antenna designs are mostly based on experience and simulations to continuously modify the relevant parameters, which is time consuming and arduous. As a machine learning algorithm, genetic algorithms have been widely used in antenna design to search for large-scale, nonintuitive solution space and find the optimal parameter value. In [12], a genetic algorithm was used to optimize the structure and length of a wire antenna. In [13], an improved hierarchical Bayesian optimization algorithm was applied to the optimization of the antenna array feed network. However, the single-objective genetic algorithms used in the above-mentioned research may not be suitable for real situations because it over-emphasizes the importance of one metric. To solve this problem, we use a multiobjective genetic algorithm to optimize the antenna by using gain, side lobe, return loss, and voltage standing wave ratio (VSWR) as objective functions.

The remainder of this paper is organized as follows. Section 2 introduces the ambient backscatter communication model and the use of the directional antenna to achieve physical layer security. Section 3 illustrates the structure of the proposed antenna and the optimization process of the multiobjective genetic algorithm. Section 4 presents the simulation and optimization results of the antenna structure, followed by Section 5, which concludes the paper.

2. System Model

Ambient backscatter has become a promising option for self-sustainable communication systems because of its energy-saving features, and has good potential for widespread use in the IoT. A typical ambient backscatter system includes an ambient source, a passive tag, and a reader, as illustrated in Figure 1.

The communication process within the tag is as follows. When an ambient source broadcasts signals to its legacy users, such as mobile phones and laptops, the tag can harvest the RF energy from the signals and use the collected energy to power the entire system. Then the micro-controller in the system tunes the variable impedance based on the signal to indicate bit "1" or "0" by backscattering or absorbing the ambient signals [14, 15]. Finally, the reader decodes the backscattered signals and recovers the two information bits, completing the tag-to-reader communication.

Evaluating the security of the system and selecting an appropriate solution improves the security of the system. A

directional antenna designed for the tag is an effective means to achieve beamforming in the IoT scenario.

2.1. Ambient Backscatter System and Signal Detection. In ambient backscatter systems, the detection of the received signal plays a vital role. Without loss of generality, we denote h_{st}, h_{sr}, and h_{tr} as gains of the channels from the source to the tag, from the source to the reader, and from the tag to the reader, respectively. We assume that $s(n)$ represents the RF source signals with zero mean and unit variance. The power of the ambient source is P_s and is unknown to the receiver. The received signal at the tag is expressed as

$$y_t(n) = \sqrt{P_s} h_{st} s(n) + w_t(n) \tag{1}$$

where $w_t(n)$ is the noise inside the tag which can be ignored because here and the tag is a passive component, i.e., $w_t(n) = 0$ [16].

The signal backscattered by the tag is

$$x_t(n) = \eta x(n) y_t(n) \tag{2}$$

where $x(n) \in \{0, 1\}$ controls the working condition of the tag antenna. The tag reflects the signal when $x(n) = 1$, and the tag does not reflect when $x(n) = 0$. $\eta \in [0, 1]$ is the attenuation factor inside the tag. The signal received at the reader is

$$\begin{aligned} y_r(n) &= h_{sr} s(n) + h_{tr} x_t(n) + w(n) \\ &= \begin{cases} \sqrt{P_s} h_0 s(n) + w(n) & x(n) = 0 \\ \sqrt{P_s} h_1 s(n) + w(n) & x(n) = 1 \end{cases} \end{aligned} \tag{3}$$

where $h_0 \triangleq h_{st}$, $h_1 \triangleq h_{sr} + \eta h_{st} h_{tr}$, and $w(n)$ is the additive white Gaussian noise (AWGN) with zero mean and σ_w^2 variance.

In ambient backscatter systems, the amplitude or phase of the backscattered signals always carries the required information.

According to amplitude or phase modulation, the main task of the backscatter reader is to determine the amplitude or phase variation. In most cases, demodulation from backscattered waves with the binary amplitude modulation requires envelope detection at the receiver. Alternatively, phase demodulation is based on phase detection. Common methods of phase demodulation include the use of a homodyne receiver with an RF in-phase/quadrature demodulation and channel estimation [17]. Subsequently, the demodulator can acquire the information bit modulated on the phase by utilizing the channel estimation value.

The conventional detection scheme of the reflected signals uses preamble packets as thresholds for detection. In recent years, many other detection schemes have been developed. For example, a detector based on differential encoding can finish the detection without the knowledge of the channel state information (CSI) [18]. A joint-energy detection scheme requires only the channel variances without requiring the specific CSI and recently, a maximum-likelihood (ML) detector has been commonly used.

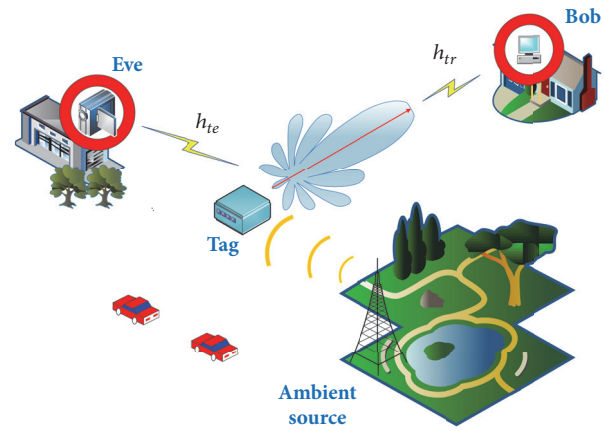


Figure 2: Wiretap channel model.

2.2. Security Assessment. Since the hardware of the tag limits the signal processing capability, the security of communication becomes a challenge for the IoT. Traditional encryption technology that relies on high computational complexity does not meet the requirements of the IoT application scenario. Beamforming, AN, cooperative interference, differential channel estimation, and network coding have become common physical layer security solutions. Among them, beamforming technology is most suitable for IoT security and allows wireless signals to propagate only in specific directions.

As shown in Figure 2, the data in the tag are modulated into the ambient carrier and the information signal is received by the legal receiver Bob over the "main channel," whereas it is received by the eavesdropper Eve over an additional "wiretap channel."

The secrecy capacity is used to measure the security of the system. In the wiretap channel, the secrecy rate is a transmission rate that can be reliably transmitted on the main channel but cannot be transmitted on the eavesdropping channel. In the case of one eavesdropper, the secrecy capacity is

$$R_s = \max\{R_d - R_e\} \tag{4}$$

where R_d is the communication rate of the source-destination link and R_e is the communication rate of the source-eavesdropper link. Usually, it is calculated as the difference between the mutual information in the primary and eavesdropping channels: $I(A; B) - I(A; E)$.

In the case of multiple eavesdroppers, the secrecy capacity is

$$R_s = \max \min_j \left\{R_d - R_e^j\right\} \tag{5}$$

The secrecy outage probability is another important variable in physical layer security communication. It is the likelihood that the instantaneous secrecy rate R_s is below a predefined threshold ε for a particular fading distribution.

$$P_{out} = P\{R_s < \varepsilon\}, \quad \varepsilon > 0 \tag{6}$$

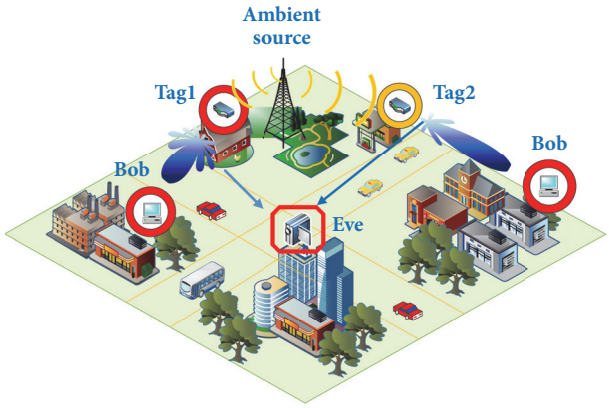


Figure 3: Influence of antenna side lobes on communication.

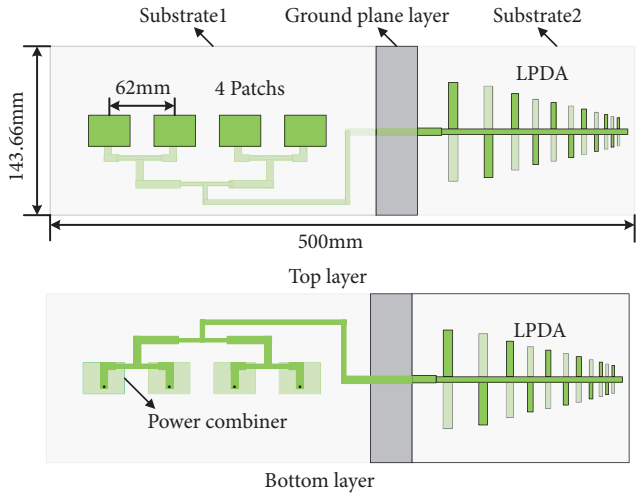


Figure 4: Dual-antenna system structure.

An analysis from the perspective of information theory indicates that the mutual information depends on the SNR of the received signal, which indicates that the secrecy capacity is determined by the SNR of the legal receiver and of the eavesdropper [19].

By using beamforming at the tag, we change the direction of the antenna to increase the gain of the main channel and reduce the signal strength of the wiretap channel by reducing the side lobes. In this way, the security of the system is enhanced and the secrecy capacity is improved, as well.

2.3. Antenna Demand. In the IoT application scenario, in order to achieve beamforming and meet the constraints of limited hardware, we designed a directional antenna with high gain and small side lobes to be used in the tag.

The previous discussion shows that providing different SNRs for eavesdroppers and readers is a key task to improve communication security. The directional antenna increases the peak gain of the antenna, thereby improving spatial reuse and expanding the geographic coverage in a given direction [20]. Moreover, the use of directional antennas improves the wireless network capacity, avoids physical jamming attempts, enhances data availability, and suppresses interference from neighbors. In addition, the antenna is required to have fewer side lobes.

We can observe in Figure 3 that Tag1 has more side lobes than Tag2 and higher side lobe levels. When the side lobes are small, the main lobe has a large transmit power, which maximizes the signal power in the desired direction while suppressing signals in undesired directions. Thus, a goal can be achieved to maximize the ratio of the SNRs received by the reader and the eavesdropper.

In addition, higher frequency signals experience several orders of magnitude of free space path loss and, therefore, communication coverage is small. By using a small sidelobe antenna, we can increase the transmission distance in the specified direction.

In order to achieve these goals, we designed a dual-antenna system consisting of a patch antenna array and a printed LPDA. The patch antenna receives the RF signal from all directions and the LPDA is directed at the reader. In addition, we use a multiobjective genetic algorithm to optimize the antenna side lobes, reduce the peak value of the largest side lobes, and enhance the directionality of the antenna.

The designed antenna does not require additional power, which prevents the disadvantages of traditional physical layer security technology. The specific structure of the antenna is described in detail in Section 3.

3. Antenna Design and Optimization

3.1. Antenna Model. The antenna system structure on the tag is shown in Figure 4 and is located on the XOY plane. The system consists of three components: a four-element patch antenna array, a feeding network, and a printed LPDA. Taking into account the receiving range and antenna gain, the receiving plane uses a simple coaxial probe-fed patch antenna. It is located on the top layer. The feed network consisting of the power combiner and the corresponding substrate is located on the bottom layer and shares the ground plane with the patch antenna array. The patch antennas coaxial probe is connected to the four input ports of the power combiner through two layers of substrate and a ground plane. The printed LPDA acts as a transmit antenna and is connected to the output port of the combiner. The total size of this dual-antenna system is $500 \times 143.66 \times 8.175 mm^3$. It is evident from the reciprocity of the antenna that when the incident wave is irradiated from the +z direction to the four-element patch antenna array, the received electromagnetic wave is transmitted to the printed LPDA through the feed network for reradiation with polarization transition characteristics, thereby changing the incident wave transmission direction and achieving the function of omnidirectional reception and directional transmission.

3.2. Calculation of the Antenna Initial Size

3.2.1. Receiving Antenna. Because high gain is a priority, a rectangular patch antenna fed by a coaxial probe is used as

the receiving antenna for the dual-antenna system. A Rogers TMM4 with a dielectric constant $\varepsilon_r = 4.5$ is chosen as the substrate with a thickness of 5 mm. According to the empirical formula provided in [21], the initial length W and width L of the patch are calculated as

$$L = \frac{c}{2f_0}\frac{1}{\sqrt{1/\varepsilon_e}} - 2\Delta L \tag{7}$$

$$W = \frac{c}{2f_0}\left(\frac{\varepsilon_r + 1}{2}\right)^{1/2} \tag{8}$$

where c is the speed of light, f_0 is the resonant frequency, h is the thickness of the substrate, ε_r is the dielectric constant of the substrate, and ε_e is the effective dielectric constant. ε_e and ΔL are calculated using the following formula:

$$\varepsilon_e = \frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2}\left(1 + 12\frac{h}{L}\right)^{1/2} \tag{9}$$

$$\Delta L = 0.412h\frac{\left(\varepsilon_e + 0.3\right)\left(W/h + 0.264\right)}{\left(\varepsilon_e - 0.258\right)\left(W/h + 0.8\right)} \tag{10}$$

The position of the feed point can be calculated by

$$X_f = \frac{L}{2\sqrt{\varepsilon_e}} \tag{11}$$

Considering the mutual coupling effect between the patches, the interval between the adjacent units is $0.5\lambda_g \sim \lambda_g$.

The four-element rectangular patch antenna array is fed in parallel by a 1-4 power combiner. The distances from the input port to every unit are equal to achieve the same phase feed.

3.2.2. Transmitting Antenna. An LPDA is a wideband antenna. In order to make the tag structure more compact, a flat printed structure is used to integrate the transceiver antennas into one plane. The structure of the printed LPDA is shown in Figure 5. The length of the antenna element is denoted by L_n and the extension of the end of each antenna element intersects at a point, called a virtual vertex, with an opening angle of α. The vertical distance from the virtual vertex to each antenna element is represented as R_n, the vibrator width is represented as w_n, and the adjacent two vibrators are separated by d_n.

The geometry of the antenna is determined by the geometric factor τ and the spacing factor σ.

$$\tau = \frac{h_{n+1}}{h_n} = \frac{L_{n+1}}{L_n} = \frac{d_{n+1}}{d_n} \tag{12}$$

$$\sigma = \frac{d_n}{4h_n} \tag{13}$$

The number of antenna elements is obtained by the following formula:

$$N_a = 1 + \frac{lg\left(K_2/K_1\right)}{lg\tau} \tag{14}$$

where K_1 and K_2 are the cutoff coefficients.

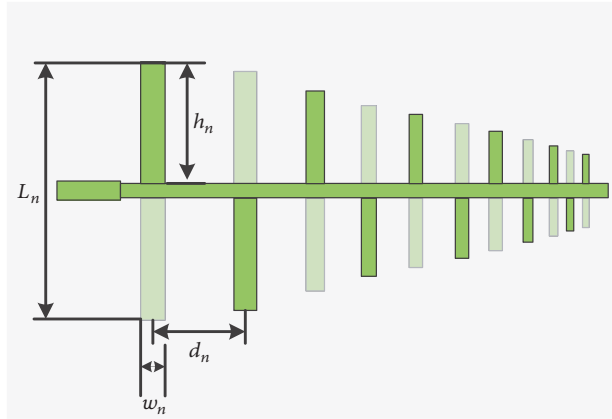


Figure 5: The structure of the printed LPDA.

$$K_1 = 1.01 - 0.519\tau \tag{15}$$

$$K_2 = 7.01\tau^3 - 21.3\tau^2 + 21.98\tau - 7.30 + \sigma\left(21.82 - 66\tau + 62.12\tau^2 - 18.29\tau^3\right) \tag{16}$$

In addition, it is necessary to estimate the width of the elements as follows:

$$Z_a \approx 120\ln\left(\frac{h}{a}\right) - 2.25 \tag{17}$$

where h/a is the half-height-to-radius ratio of the dipole. In the planar printing structure, we use microstrip patches instead of cylindrical dipoles. Considering the equivalent perimeters of the cylindrical and thin rectangular conductors, we used the approximate relationship $w \approx \pi a$, where Z_a represents the average characteristic impedance, which is 50Ω here. w represents the dipole width.

The LPDA is an end-fire antenna and the maximum radiation direction is from the longest oscillator to the shortest oscillator [22]. When the operating frequency changes, the radiation area of the antenna moves around the antenna and maintains similar characteristics; therefore, the pattern of the antenna changes little with the frequency. In general, the larger the value of τ, the higher the number of oscillators in the radiation region, the stronger the directivity of the antenna, and the smaller the half-power angle of the pattern. The lengths of the longest oscillator and the shortest oscillator of the LPDA determine the operating frequency.

The LPDA is a linearly polarized antenna. When the LPDA's oscillator plane is placed horizontally, it radiates or receives horizontally polarized waves; when its oscillator plane is placed vertically, it radiates or receives vertically polarized waves. Circular polarization is easier to achieve with a planar structure.

3.2.3. Optimization Scheme. Since the directional antenna has a larger impact on the physical layer security and the structure of the LPDA is more complex, the transmitting antenna is optimized. We select the lengths, widths, and spacings of the elements as variables for the optimization.

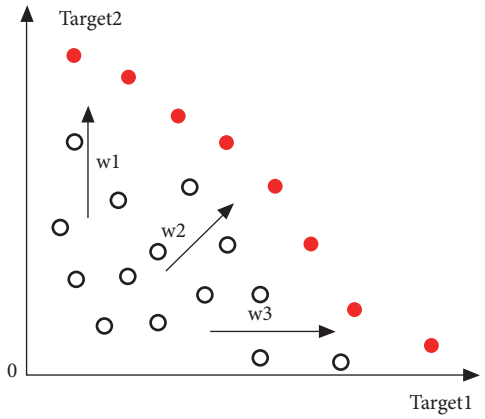


Figure 6: Pareto front.

During the design of the antenna, the gain, bandwidth, side lobes, and standing wave ratio (VSWR) of the antenna are important indicators of the performance of the antenna. Therefore, the function corresponding to the abovementioned four indicators is defined as the objective function.

In the actual design process of the antenna, there are usually multiple targets that need to be optimized. There may be contradictory relationships between the various objectives, and it is impossible to achieve optimality at the same time. Therefore, a multiobjective genetic algorithm (MOGA) was introduced.

In MOGA, there exists a set of Pareto-optimal or nondominated solutions generating a set of Pareto-optimal outcomes/objective vectors, which is called pareto front. Explicitly, the pareto front is generated by the specific set of solutions, for which none of the multiple objectives can be improved without sacrificing the other objectives, as shown in Figure 6.

A traditional multiobjective optimization scheme uses a method of assigning weights to convert multiple goals into a single goal. However, due to the nonconcaveness of multiobjectives, in order to find the Pareto front, a three-dimensional search is required for each weight $\overline{w} = [w_1, w_2, w_3]$, which is very time-consuming. Moreover, as the number of objective functions increases, the complexity of the weighting method is greatly increased. In addition, it is challenging to assign weights to each decision variable. Therefore, a new optimization solution is needed.

In this study, a multiobjective genetic algorithm (MOGA) is introduced as an optimization scheme, namely, the nonsorting genetic algorithm (NSGA)-II. The NSGA-II is considered one of the classic MOGAs. The algorithm obtains a potential uniformly distributed Pareto optimal solution set by fast nondominated sorting, crowded degree calculation, and an elitism strategy. This is very helpful for improving the exploratory capacity of the NSGA.

The specific process is shown in Figure 7.

The NSGA-II first finds nondominated solutions in the population and stratifies the population through nondominated sorting. Subsequently, these points are removed and identified and the nondominated solutions in the remaining population are removed. The algorithm updates the current

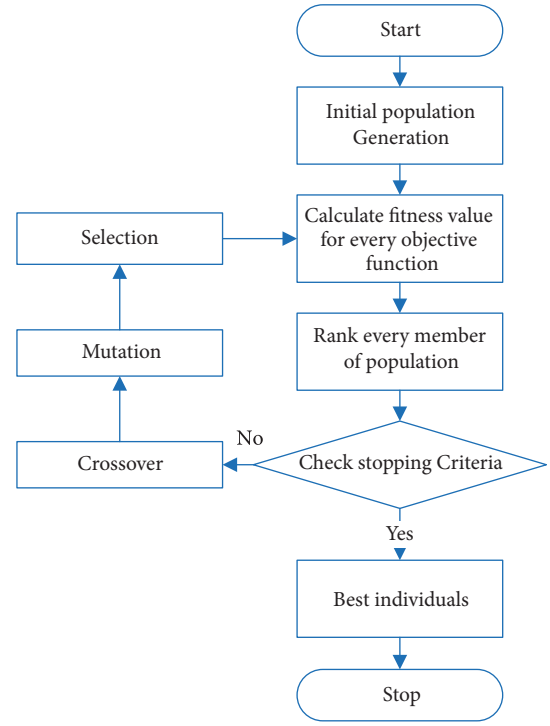


Figure 7: Flowchart of the MOGA.

archive by identifying the old archive and all current nondominated solutions in the aggregate. These layers are used in turn until the maximum archive is reached. The point closest to the target value is obtained by considering the crowding distance operator.

Unlike traditional optimization methods, MOGAs do not convert multiple targets into a single target for optimization using weighting but seek to optimize multiple targets simultaneously. Thereby, an optimal solution set can be found that satisfies multiple goals.

3.2.4. Decision Variables. A multiobjective optimization problem with three decision variables and four objective functions is expressed as

$$Optimal\overline{F}(\overline{x}) = [F_1(\overline{x}), F_2(\overline{x}), F_3(\overline{x}), F_4(\overline{x})] \quad (18)$$

where $\overline{F}(\overline{x})$ is the vector of the objective functions. $F_1(\overline{x}), F_2(\overline{x}), F_3(\overline{x}), F_4(\overline{x})$ represent the objective functions, where $\overline{x} = [L_1, L_2, \ldots, L_n, d_1, d_2, \ldots, d_n, w_1, w_2, \ldots, w_n]$.

Here, X and Z represent the search space and the target space, respectively. Thus, using the mapping $\overline{F} : X \longrightarrow Z$ each vector $\overline{x} \in X$ corresponds to a vector $\overline{z} = \overline{F}(\overline{x}) \in Z$.

We ensure that the height of the high-order oscillator is greater than the length of the low-order oscillator. All are within the appropriate range. According to the physical meaning of the variable, its optimization range is given as $L_i \in [5, 40]$, $d_i \in [1, 15]$, $w_i \in [0.1, 3]$ (unit: mm).

3.3. Objective Function

3.3.1. Bandwidth. The objective function is designed to increase the antenna bandwidth so that the transmit antenna

can operate over a wider frequency range. The target frequency band is determined by a $10dB$ return loss S_{11} and ranges from $2GHz$ to $4GHz$. Therefore, the fitness function is defined as the average of the return loss of less than $-10dB$ in the frequency band.

$$F_1(\overline{x}) = \frac{1}{N}\sum_{i=1}^{N} Q(f_i) \tag{19}$$

$$Q(f_i) = \begin{cases} 10 & S_{11} < -10 \\ |S_{11}(f_i)| & S_{11} \geqslant -10 \end{cases} \tag{20}$$

In the above equation, f_i is the sampling frequency. If the average value of S_{11} at the sampling frequency is less than $-10dB$, it is concluded that the design goal has been achieved.

In the design example, we set the parameters as follows:

The sampling frequency is $N = 5$; $f_1 = 2GHz$, $f_2 = 2.5GHz$, $f_3 = 3GHz$, $f_4 = 3.5GHz$, and $f_5 = 4GHz$. When $F_1(x) \geqslant 10$, the objective function is satisfied.

3.3.2. VSWR. The VSWR is an important indicator to measure the antenna matching state; the VSWR is limited to $[1, 1.8]$

$$VSWR(f_i) = \begin{cases} VSWR & VSWR \leqslant 1.8 \\ 1.8 & VSWR < 1.8 \end{cases} \tag{21}$$

$$F_2(\overline{x}) = \frac{1}{N}\sum_{i=1}^{N} VSWR(f_i) \tag{22}$$

where $N = 5$ is the number of sampling points of $2 \sim 4GHz$. When $F_2(x) \leqslant 1.8$, the objective function is satisfied.

3.3.3. Gain. The antenna gain is a measure of the ability of an antenna to transmit and receive signals in a specific direction. It is an important indicator used for antenna optimization. The average gain in the band is used as the objective function:

$$F_3(\overline{x}) = \frac{1}{N}\sum_{i=1}^{N} Gain(f_i) \tag{23}$$

3.3.4. Side Lobes. Since the antenna has many side lobes, the maximum side lobes tend to have a level that is not much different from the maximum gain of the antenna. In the physical layer security, there is a strict requirement for the orientation of the antenna and it is necessary to reduce the peak value of the highest side lobes as much as possible. This is required because if the eavesdropper is located in the direction of the largest side lobe, information leakage may occur. Therefore, the optimization goal is the minimization of the maximum peak of the side lobes.

The total radiation pattern factor $f(\theta, \phi)$ of the M cells of the LPDA shown in Figure 4 is

$$\begin{aligned} f(\theta,\phi) &= \sin\theta \sum_{p=1}^{M} L_p \\ &\cdot \exp\left[jk\left(X_p \sin\theta\cos\phi + Y_p \sin\theta\sin\phi + Z_p\cos\theta\right)\right] \\ &\cdot \sum_{n=1}^{N} (-1)^n \times \frac{(2n-1)\, L_{np} \cos\left(\pi L_p \cdot \cos\theta\right)}{(2n-1)^2 - \left(2L_p \cdot \cos\theta\right)^2} \end{aligned} \tag{24}$$

The optimization goal is min $F_4(\overline{x})$, subject to

$$F_4(\overline{x}) = \max_{f_i \in [2GHz, 4GHz]} \left(SLL(f_i)\right) \tag{25}$$

3.3.5. Fuzzy Decision Making. Fuzzy set theory is a method to find the optimal compromise solution from the Pareto front. Using linear fuzzy membership function modeling, the objective function value is mapped to the satisfaction function. This defines a linear membership function sf_n

$$sf_n = \begin{cases} 1 & if\ z_n \geqslant z_n^{max} \\ 1 - \dfrac{z_n^{max} - z_n}{z_n^{max} - z_n^{min}} & if\ z_n^{min} < z_n < z_n^{max} \\ 0 & if\ z_n \leqslant z_n^{min} \end{cases} \tag{26}$$

where z_n^{min} and z_n^{max} are the minimum and maximum values of the $n - th$ objective function respectively. The canonical membership function of the $n - th$ nondominated solution of the objective function is expressed as

$$s_j = \frac{\sum_{n=1}^{N_{obj}} sf_n^j}{\sum_{j=1}^{M_{par}} \sum_{n=1}^{N_{obj}} sf_n^j} \tag{27}$$

where N_{obj} represents the number of objective functions and M_{par} is the number of nondominated solutions in the Pareto front. We choose the solution vector with the maximum s_j value as the optimal compromise solution.

4. Numerical Results

The design examples and results are provided in this section and represent the optimal design of the LPDA based on the multiobjective genetic algorithm.

The signals in the domestic environment are mainly composed of four types: WiFi signals, terrestrial digital TV broadcast signals, mobile 4G signals, and upcoming 5G signals which has ultra-high spectrum utilization and ultra-low power consumption and will be widely used in the future. Considering the requirements of the signal coverage in various environments, transmission rate, signal stability, security, signal spectrum, and transmission power, a working frequency band of $2GHz \sim 4GHz$ is used in order to meet the requirements of IoT communications. The antenna design goals are shown in Table 1.

According to the design optimization scheme, 35 variables are selected as the optimization variables, including the length $L_1 \sim L_{12}$, the width $w_1 \sim w_{12}$, and the spacing $d_1 \sim d_{11}$ of the elements. The optimization ranges $L_i \in [5, 40]$, $d_i \in [1, 15]$, and $w_i \in [0.1, 3]$ (unit: mm) are used.

Table 1: Antenna design index.

Index	Value
Working frequency	$2GHz \sim 4GHz$
Maximum VSWR in the band	< 2
Average VSWR	< 1.3
Minimum gain in the band	$> 5dB$
Average gain	$> 6.5dB$
Maximum side lobe level	$< -4dB$
Return loss (S_{11})	$< -10dB$
Antenna size	$< 30cm$

Table 2: Simulation parameter optimization (unit: mm).

L_1	L_2	L_3	L_4	L_5	L_6	L_7
36	32.4	29.16	26.24	23.62	21.26	19.2
L_8	L_9	L_{10}	L_{11}	L_{12}	d_1	d_2
17.22	15.50	13.95	12.55	11.30	13	11.7
d_3	d_4	d_5	d_6	d_7	d_8	d_9
10.53	9.48	8.53	7.68	6.91	6.22	5.60
d_{10}	d_{11}	Gain	SLL			
5.04B	4.53	$7.0dB$	$-5.76dB$			

Based on a large number of simulation calculations, we chose the NSGA-II algorithm to optimize the antenna parameters. We set the population size to 100, the maximum number of iterations to 250, the crossover probability to $p_c = 0.7$, and the mutation probability to $p_m = 1/n_{var}$, where $n_{var} = 35$ is the number of decision variables. The frequency is sampled at intervals of $500MHz$ in the $2GHz$ to $4GHz$ band. After iterative optimization, the antenna parameters were obtained and are shown in Table 2.

The criteria for measuring the quality of an algorithm are time complexity and space complexity. Time efficiency refers to the execution time of the algorithm. Regarding the computational complexity of genetic algorithms, Goldberg et al. proposed the concept of takeover time to discuss the time complexity of the algorithm [23]. In the antenna design of this paper, the time complexity is defined as the calculation time, i.e., the number of iterations it takes to find an optimal solution, which is more practical.

The genetic algorithm can end with convergence or end with the number of iterations [24]. After several iterations, the results began to stabilize. Therefore, this paper selects 250 iterations as the end condition. At this point each target meets the design requirements.

An excitation source is used to stimulate the receiving and transmitting antennas at the same time to simulate the overall gains G_1 and G_2. A pattern of the LPDA antenna at a center frequency of $2.4GHz$ can be obtained, as shown in Figure 7. It can be seen that the planar LPDA has good directivity and can be optimized to achieve gains of $7.0dB$. The reciprocity of the antenna indicates that a certain range of electromagnetic waves received by the patch antenna is radiated through the LPDA and used as a relay antenna on the tag.

In Figure 8, a comparison of patterns before and after optimization is shown. Prior to the optimization, there are

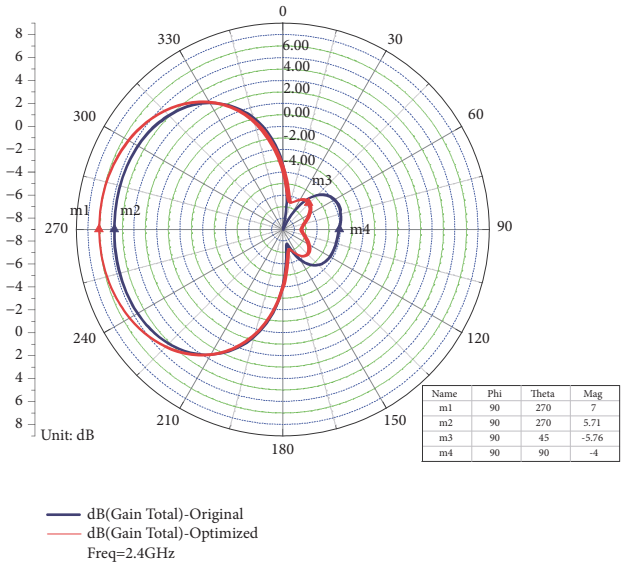


Figure 8: Gain and side lobes before and after optimization.

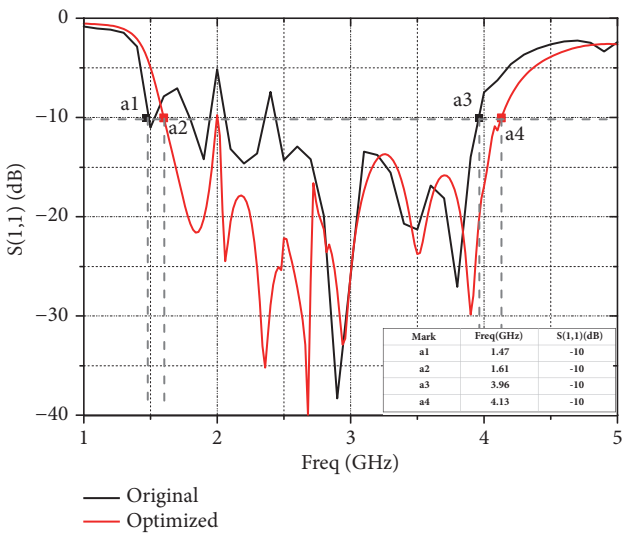


Figure 9: Return loss S_{11}.

1 large side lobes, and the maximum side lobe level is $-4dB$. After optimization, the maximum side lobes are reduced to $-5.76dB$, which effectively enhances the directionality of the antenna.

The curves shown in Figures 9 and 10 show the changes in the return loss S_{11} and the VSWR versus the frequency before and after optimization, respectively. It can be seen that the optimized $10dB$ impedance bandwidth is $2.5GHz$ and the average VSWR in the band is 1.3, reaching the expected target.

In order to prove that the designed antenna can effectively improve the security of the channel, we evaluate the channel secrecy capacity.

Assume that the ambient source power is P_t, the transmission gain is G_t, the distance from the ambient source to the tag is r_1, and the distance from the tag to the reader is r_2.

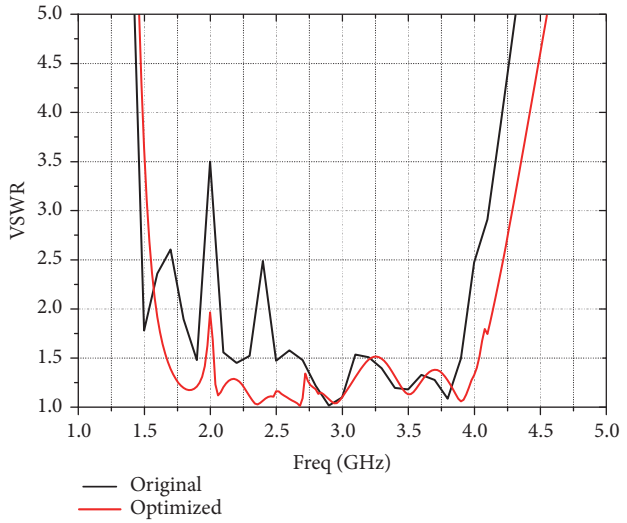


Figure 10: VSWR vs. frequency.

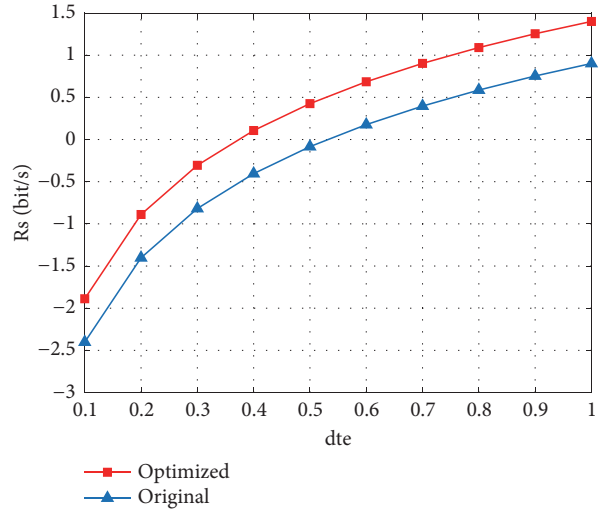


Figure 11: Secrecy capacity assessment.

From the radar equation, the signal power P_r received by the reader can be obtained as

$$P_r = \frac{P_t G_t}{4\pi r_1^2} \cdot \frac{\sigma}{4\pi} \cdot \frac{A_r}{r_2^2} \tag{28}$$

where σ is the radar cross section and $A_r = G_r \lambda_0^2 / 4\pi$ is the effective area of the receiving antenna. G_r is the gain of the reader received signal and λ_0 is the signal wavelength.

Assume that the received power of the legitimate user is P_d, the noise power received by the legitimate user is N_d, the received power of the illegal eavesdropping user is P_e, and the received noise power is N_e. R_d and R_e represent the primary channel and eavesdropping channel capacity, respectively. The secrecy capacity can be calculated as

$$R_s = R_d - R_e = \frac{1}{2} \log\left(1 + \frac{P_d}{N_d}\right) - \frac{1}{2} \log\left(1 + \frac{P_e}{N_e}\right) \tag{29}$$

where P_d and P_e can be obtained from (28). In the same communication system, each node receives the same noise, i.e., $N_d = N_e$. All simulation data were quantified and the results of the evaluation are shown in Figure 11. The abscissa d_{te} indicates the distance between the eavesdropper and the tag, and the ordinate indicates the channel secrecy capacity. After optimization, the channel secrecy capacity is increased by $0.5 bit/s$ overall.

The results indicate that the relay antenna is optimized by the multiobjective genetic algorithm; the gain is 7.0 dB and the maximum side lobe level is reduced to $-5.76 dB$, which enhances the antenna's directionality. This makes it more difficult for the eavesdropper to obtain communication information. The antenna can be safely applied in the ambient backscatter communication of the IoT.

5. Conclusion

In this study, we investigated an important communication form of the IoT, i.e., ambient backscattering, and proposed a machine learning based antenna design scheme for physical layer security. The directional communication from the relay tag to the reader is achieved by combining a patch antenna and an LPDA. In order to reduce antenna side lobes and improve orientation performance, we used a multiobjective genetic algorithm to optimize the antenna size and obtain a set of optimal Pareto fronts. The simulation results justified that our proposed antenna design has a simple structure, saves energy, and can effectively protect the physical layer IoT communications.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: wireless communication out of thin air," in *Proceedings of the the ACM SIGCOMM 2013 conference*, p. 39, Hong Kong, China, August 2013.

[2] D. T. Hoang, D. Niyato, P. Wang, D. I. Kim, and Z. Han, "Ambient Backscatter: A New Approach to Improve Network Performance for RF-Powered Cognitive Radio Networks," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3659–3674, 2017.

[3] X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han, "Ambient Backscatter Assisted Wireless Powered Communications," *IEEE Wireless Communications Magazine*, vol. 25, no. 2, pp. 170–177, 2018.

[4] C. Perez-Penichet, "Ph.D. Forum Abstract: Ambient Backscatter Communication," in *Proceedings of the 15th ACM/IEEE*

International Conference on Information Processing in Sensor Networks, IPSN 2016, Austria, April 2016.

[5] S. Han, S. Xu, W. Meng, and C. Li, "Dense-Device-Enabled Cooperative Networks for Efficient and Secure Transmission," *IEEE Network*, vol. 32, no. 2, pp. 100–106, 2018.

[6] W. Zhang, W. He, X. Chen, Y. Cai, X. Guan, and J. Qu, "Power allocation for improving physical layer security in D2D communication via stackelberg game," in *Proceedings of the 8th International Conference on Wireless Communications and Signal Processing, WCSP 2016*, pp. 1–5, Yangzhou, China, October 2016.

[7] T. Q. Duong, "Keynote talk #1: Trusted communications with physical layer security for 5G and beyond," in *Proceedings of the International Conference on Advanced Technologies for Communications (ATC)*, p. xxxiv, Quy Nhon, Vietnam, 2017.

[8] P. Zhang, Y. Ma, and B. Wang, "Improving physical layer security via multiple-level relay network," in *Proceedings of the 2014 12th IEEE International Conference on Signal Processing, ICSP 2014*, pp. 1851–1854, Hangzhou, China, October 2014.

[9] A. Mukherjee, "Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[10] Z. Chen, H. Li, G. Cui, and M. Rangaswamy, "Adaptive transmit and receive beamforming for interference mitigation," *IEEE Signal Processing Letters*, vol. 21, no. 2, pp. 235–239, 2014.

[11] Q. Chen, S.-W. Qu, J. Li, L. Wang, Q. Yuan, and K. Sawaya, "Dual-antenna system composed of patch array and planar Yagi-Uda array," in *Proceedings of the 5th European Conference on Antennas and Propagation, EUCAP 2011*, pp. 1023–1026, Rome, Italy, April 2011.

[12] E. E. Altshuler and D. S. Linden, "Wire-antenna designs using genetic algorithms," *IEEE Antennas and Propagation Magazine*, vol. 39, no. 2, pp. 33–43, 1997.

[13] S. Santarelli, T.-L. Yu, D. E. Goldberg et al., "Military antenna design using simple and competent genetic algorithms," *Mathematical and Computer Modelling*, vol. 43, no. 9-10, pp. 990–1022, 2006.

[14] W. Zhao, G. Wang, R. Fan, L. Fan, and S. Atapattu, "Ambient Backscatter Communication Systems: Capacity and Outage Performance Analysis," *IEEE Access*, vol. 6, pp. 22695–22704, 2018.

[15] Y. Liu, G. Wang, Z. Dou, and Z. Zhong, "Coding and Detection Schemes for Ambient Backscatter Communication Systems," *IEEE Access*, vol. 5, pp. 4947–4953, 2017.

[16] G. Wang, F. Gao, R. Fan, and C. Tellambura, "Ambient Backscatter Communication Systems: Detection and Performance Analysis," *IEEE Transactions on Communications*, vol. 64, no. 11, pp. 4836–4846, 2016.

[17] S. J. Thomas and M. S. Reynolds, "A 96 Mbit/sec, 15.5 pJ/bit 16-QAM modulator for UHF backscatter communication," in *Proceedings of the 2012 6th IEEE International Conference on RFID, RFID 2012*, pp. 185–190, Orlando, FL, USA, April 2012.

[18] D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti, "BackFi: High Throughput WiFi Backscatter," in *Proceedings of the 2015 ACM SIGCOMM*, London, UK, 2016.

[19] F. Zhu and M. Yao, "Improving Physical-Layer Security for CRNs Using SINR-Based Cooperative Beamforming," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1835–1841, 2016.

[20] W. X. Liu, Y. Z. Yin, W. L. Xu, and S. Zuo, "Compact open-slot antenna with bandwidth enhancement," *IEEE Antennas and Wireless Propagation Letters*, vol. 10, pp. 850–853, 2011.

[21] K. R. Carver and J. W. Mink, "Microstrip Antenna Technology," *IEEE Transactions on Antennas and Propagation*, vol. 29, no. 1, pp. 2–24, 1981.

[22] R. R. Pantoja, A. R. Sapienza, and F. C. Medeiros Filho, "A Microwave Printed Planar Log-Periodic Dipole Array Antenna," *IEEE Transactions on Antennas and Propagation*, vol. 35, no. 10, pp. 1176–1178, 1987.

[23] S. Han, S. Xu, W. Meng, and C. Li, "An agile confidential transmission strategy combining big data driven cluster and OBF," *IEEE Transactions on Vehicular Technology*, no. 99, article 1, 2017.

[24] S. Qiao, X. Dai, Z. Liu, J. Huang, and G. Zhu, "Improving the optimization performance of NSGA-II algorithm by experiment design methods," in *Proceedings of the 2012 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications, CIMSA 2012*, pp. 82–85, Tianjin, China, July 2012.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 5012096, 8 pages
https://doi.org/10.1155/2018/5012096

Research Article

Energy-Efficient Transmission Based on Direct Links: Toward Secure Cooperative Internet of Things

Xiaohui Shang, Aijun Liu, Yida Wang, Qing Xie, and Yong Wang

Department of Satellite Communications, Army Engineering University of PLA, Nanjing 210014, China

Correspondence should be addressed to Xiaohui Shang; shangxiaohui1214@126.com

Received 17 September 2018; Accepted 4 December 2018; Published 17 December 2018

Guest Editor: Dajiang Chen

In this paper, the secure uplink transmission scenario in Internet of Things (IoT) applications is investigated, where one of multiple sensors communicates with the controller aided by the cooperative relay. Firstly, by considering the direct link, an energy-efficient transmission scheme (EET) is proposed, which can be suitable for the resource-constrained devices and applications in IoT communication. Moreover, the secrecy outage probability (SOP) and secure energy efficiency (SEE) of different transmission strategies are derived, which contributes to the design of energy-efficient secure transmission. Finally, simulation results demonstrate that EET outperforms other transmission protocols in terms of SEE in most situations. To improve the secrecy performance and energy efficiency of the IoT deployment, EET can be adopted as an effective additional strategy in practical applications.

1. Introduction

The Internet of Things (IoT), serving as an important architecture in the fifth-generation (5G) mobile communication systems, has drawn dramatic interest all over the world [1–3]. However, most of IoT terminal devices are resource-constrained commonly, which causes low computing power and energy storage capacity. Generally, it is necessary for IoT applications to operate at low power. Meanwhile, since most devices are battery-powered sensor nodes that cannot be replaced for some reasons, such as being embedded in a human body, these sensors are required to work for a long time without human intervention [4]. Consequently, energy efficiency is worthy of concern in the IoT system especially.

Cooperative transmission in wireless communications has been considered as a promising solution in order to economize the power of transmitter, improve throughput, and enhance the reliability of communications [5]. Because of limited resources of IoT devices, the employment of relay transmission is of utmost importance for IoT to cope with the issue of energy efficiency. Traditional cooperative protocols have been studied deeply by many researchers [6, 7], such as amplify-and-forward (AF) and decode-and-forward (DF), in which DF can be further subdivided into fixed DF and selective DF [8], as well as cooperative jamming (CJ) [9, 10]. In particular, for the CJ scheme, the relay does not forward confidential information but emits interference signals (also known as artificial noise) to interfere with the eavesdropper. It is worth noting that a common problem in [6–10] is that the direct link between the source and the target has been unexploited.

On the other hand, it is also necessary to consider the security and privacy issues for IoT. Obviously, not all devices connected via the IoT are able to access the network data. Moreover, the wireless communication channel is open, which may also lead to the eavesdropping risk caused by unauthorized users. In general, security has always been regarded as a problem that needs to be solved by high-layer computing methods. However, physical layer security (PLS), which is an emerging method to ensure the security of wireless communication, has become an effective supplement to existing solutions. In terms of wireless PLS, the basic idea is to make use of the characteristics of wireless channels to transmit information reliably from the source to the intended receiver as well as to ensure the confidentiality of the information, that is, not to be intercepted or eavesdropped [11]. In recent years, PLS techniques have been widely explored to ensure security of future wireless communications, as it could

provide the security of new network architectures such as the IoT. Unfortunately, energy efficiency of PLS has not aroused sufficient attention in the cooperative relay networks and IoT scenario.

The measurements of PLS are generally related to the availability of channel state information (CSI) for source. When the source well knows global CSI, the confidential information will not leak to the eavesdropper via the adaption of secure coding rate; thus the so-called perfect secrecy can be realized [12]. In this case, the measurement of security is secrecy capacity [13–15]. However, the hypothesis of knowing global CSI is too strong to be realized easily, since it may require the intended destination to report its information of the position; in addition, eavesdroppers collaboration to give feedback on CSI to the source is also required. Obviously, above requirement may be not suitable for the IoT devices because it will lead to higher cost and power consumption as well as more serious latency, which are unacceptable to the effective deployment of massive IoT. Therefore, a more realistic way of applying the probabilistic view is proposed, in which it was assumed that only part of the CSI of the legitimate channel is known and communication operates at a fixed secure transmission rate. At this point, security is denoted by the secrecy outage probability (SOP) [16].

Inspired by previous work, this paper focuses on secure uplink transmission scenario in IoT applications, in which one of multiple sensors in the localized group transmits collected data to a controller aided by the cooperative relay when considering the presence of a passive eavesdropper. A more practical scenario worthy of concern is that there exists a direct link between controller and sensor. With the optimal performance and controllable cost, MRC technique is usually utilized by controller to process the received signal [17]. The main contributions of this work are listed below.

(1) By making use of the advantages of both direct and relay links, we propose a novel energy-efficient secure transmission strategy based on the CSI of the legitimate link, that is, energy-efficient transmission (EET), by which the best path is selected (direct or cooperative transmission), to cope with implementation limits of the IoT devices. Since the source has known about CSI of main links, then the direct or cooperative transmission could be performed based on the above information, which contributes to decreasing energy consumption and improving secure energy efficiency (SEE).

(2) We obtain the closed-form expressions of SOP and SEE, which will be helpful to secure the applications of cooperative IoT. In order to show the effectiveness of our new strategy, we further compare the secrecy performance of different transmission schemes such as EET, DF, AF, and CJ as well as direct transmission (DT).

(3) Our results demonstrate that the proposed EET is superior to other transmission protocols in many cases when considering SEE. To improve the secrecy performance and energy efficiency of the IoT deployment with the help of cooperative relay, EET can be regarded as an effective additional strategy in practical applications.

This paper is organized as follows. In Section 2, we present the system model and our EET design. The exact SOP and SEE of proposed strategy and DT as well as other conventional cooperative protocols are derived in Section 3. Then the secrecy performance of above transmission strategies is shown by simulation results in Section 4. Finally, conclusions of this paper are drawn in Section 5.

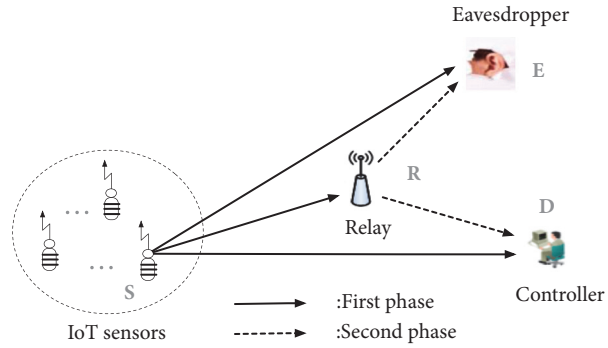


Figure 1: System model.

2. System Model and EET Design

2.1. System Model and Notation. Figure 1 shows the communication model of a single-antenna IoT device in the presence of wireless cooperative links, where one of multiple IoT sensors (S) transmits the detected data to a desired controller (D) aided by a relay (R) when considering the presence of a passive eavesdropper (E). This model can use the direct link to improve the reliability of the system [18]. The helper node, which is adopted as a relay or as a jammer, is equipped with a single antenna used for data transmission and reception in a half-duplex manner. The signal received by any node $j \in (\mathrm{R}, \mathrm{D}, \mathrm{E})$ from the transmitting terminal of $i \in (\mathrm{S}, \mathrm{R})$, $i \neq j$, is expressed as

$$y_{ij} = \sqrt{k_{ij} P_i} h_{ij} x_i + n_{ij} \tag{1}$$

where we denote k_{ij} as the path-loss between nodes i and j, P_i as the transmit power of i, x_i as the useful data signal, and n_{ij} as the zero-mean and variance $N_0/2$ additive white Gaussian noise (AWGN). Furthermore, we denote h_{ij} as the channel coefficient between nodes i and j, which exhibits Rayleigh flat-fading that remains constant for the duration of one transmission block time and varies in different block independently. Assuming that all wireless channels are independent and distributed as exponential random variables, the receiver can fully obtain the CSI of legitimate link [19]. Consequently, the intended end can obtain CSI of the main links. It is reasonable due to the fact that R and D can get available channel parameters of the main link with the assistance of channel estimation; then D is able to attain accurate CSI through cooperative relays [20]. The path-loss is $k_{ij} = G\lambda^2/4\pi^2 d_{ij}^{v} M_l N_f$, where G is the total antenna gain, λ denotes the wavelength, d_{ij} represents the distance between nodes i and j, v is the path-loss exponent, M_l denotes the link margin, and N_f is the noise at the intended receiver. Next, the instantaneous signal-to-noise ratio (SNR) at any $i-j$ channel can be expressed as $\gamma_{ij} = |h_{ij}|^2 \overline{\gamma}_{ij}$, where $\overline{\gamma}_{ij} = k_{ij} P_i / N$

represents the average SNR, $N = N_0B$ is defined as the noise power and B denotes the channel bandwidth, and any γ_{ij} is exponentially distributed according to the probability density function (PDF) $f_{\gamma_{ij}} = (1/\gamma_{ij})e^{-\gamma_{ij}/\overline{\gamma}_{ij}}$ for $\gamma_{ij} > 0$.

In line with [13], the achievable secrecy rate of source-destination (C_S) is given by

$$C_S = [C_L - C_E]^+ \tag{2}$$

$$C_L = \frac{1}{2}\log(1+\gamma_L) \tag{3}$$

$$C_E = \frac{1}{2}\log(1+\gamma_E) \tag{4}$$

where C_L denotes the capacity of the legitimate link and C_E represents the capacity of the eavesdropper link, γ_L and γ_E are the end-to-end instantaneous SNR of the legitimate and eavesdropper links, respectively, and $[x]^+ \triangleq \max\{0, x\}$.

2.2. EET Design. For the EET strategy, the selection criterion is that the sensor determines the most secure method (the direct or cooperative transmission) to be transmited to D with the aid of the available CSI. Different from the conventional cooperative protocols, since we consider both the direct and relay links simultaneously, the proposed EET can achieve better security performance. Then, in ETT, the capacity of the legitimate channel can be described by

$$C_L^{ETT} = \frac{1}{2}\max\left\{\overbrace{\log_2(1+2\gamma_{SD})}^{C_{L_{dir}}}, \underbrace{\min\{\log_2(1+\gamma_{SR}), \log_2(1+\gamma_{SD}+\gamma_{RD})\}}_{C_{L_{coop}}}\right\} \tag{5}$$

It is worth noting that the term 1/2 in (5) denotes the half duplexing cost. Then, the corresponding secrecy capacity of EET is expressed as $C_S^{EET} = [C_L^{EET} - C_E^{EET}]^+$, where C_E^{EET} is obtained from (5) by replacing D by E.

3. Secrecy Performance Analysis

We resort to the SOP and SEE to analyze the secure performance for EET as well as DT, DF, AF, and CJ protocols in this section.

3.1. Secrecy Outage Probability. In the following, the SOP can be formulated as

$$P_{out}^{sch} = \Pr\left\{C_S^{sch} < R_S\right\} = \Pr\left\{C_L^{sch} - C_E^{sch} < R_S\right\} \tag{6}$$

where $sch \in$ EET, DT, DF, AF, and CJ.

3.1.1. Derivation for EET. In general, the relay R is located in the middle position of the source S and the controller D, and we make the following considerations to (5): S (or the relay R) transmits data when $\gamma_{SD} \geq \gamma_{SR}$ (or when $\gamma_{SR} > \gamma_{SD}$). Based on the fundamental principle of EET, SOP can be expressed by

$$P_{out}^{EET} = \overbrace{\Pr\left\{C_{L_{dir}}^{EET} - C_{E_{dir}}^{EET} < 2R_S \cap \gamma_{SD} \geq \gamma_{SR}\right\}}^{p_{dir}} + \underbrace{\Pr\left\{C_{L_{coop}}^{EET} - C_{E_{coop}}^{EET} < 2R_S \cap \gamma_{SR} > \gamma_{SD}\right\}}_{P_{coop}} \tag{7}$$

where p_{dir} is obtained as

$$\begin{aligned} p_{dir} &= \Pr\left\{\left(\frac{1+2\gamma_{SD}}{1+2\gamma_{SE}}\right) < 2^{2R_S} \cap \gamma_{SD} \geq \gamma_{SR}\right\} \\ &= \Pr\left\{\gamma_{SE} > \Delta \cap \gamma_{SD} \geq \gamma_{SR}\right\} \end{aligned} \tag{8}$$

where $\Delta \triangleq (2^{-2R_S}(1+2\gamma_{SD})-1)/2$. For the Rayleigh fading, γ_{SD} and γ_{SR} are random variables that follow the exponential distribution, and their PDFs have been given above; thus,

$$\begin{aligned} p_{dir} &= \int_0^{\infty}\int_0^{\gamma_{SD}}\int_{\Delta} f_{\gamma_{SD}} f_{\gamma_{SR}} f_{\gamma_{SE}} d\gamma_{SE} d\gamma_{SR} d\gamma_{SD} \\ &= \frac{2^{4R_S}\overline{\gamma_{SD}}\,\overline{\gamma_{SE}}\exp\left(\left(1-2^{-2R_S}\right)/2\overline{\gamma_{SE}}\right)}{\left(\overline{\gamma_{SD}}+2^{R_S}\overline{\gamma_{SE}}\right)\left[\overline{\gamma_{SD}}\,\overline{\gamma_{SR}}+2^{2R_S}\overline{\gamma_{SE}}\left(\overline{\gamma_{SD}}+\overline{\gamma_{SR}}\right)\right]} \end{aligned} \tag{9}$$

When the sensor decides to utilize the relay, we consider that $\gamma_D = \gamma_{SD} + \gamma_{RD}$ and $\gamma_E = \gamma_{SE} + \gamma_{RE}$ are the SNRs at D and E, respectively, and their PDFs are expressed by $g_{\gamma_i} = g_{\gamma_{Si}+\gamma_{Ri}} = (1/(\overline{\gamma_{Ri}} - \overline{\gamma_{Si}}))(e^{-\gamma_i/\overline{\gamma_{Ri}}} - e^{-\gamma_i/\overline{\gamma_{Si}}}), i \in \{D, E\}$. Then, the SOP yields in the following cases

$$\begin{aligned} p_{coop} &= \overbrace{\Pr\left\{\frac{1+\gamma_{SR}}{1+\gamma_E} < 2^{2R_S} \cap \gamma_{SR} < \gamma_D \cap \gamma_{SR} > \gamma_{SD}\right\}}^{p_1} \\ &\quad + \underbrace{\Pr\left\{\frac{1+\gamma_{SR}}{1+\gamma_E} < 2^{2R_S} \cap \gamma_{SR} \geq \gamma_D \cap \gamma_{SR} > \gamma_{SD}\right\}}_{p_2} \end{aligned} \tag{10}$$

To obtain p_1, we isolate γ_E and use the integral that $\int_{\gamma_{SD}}^{\gamma_D} f_{\gamma_{SR}} d\gamma_{SR} = \int_0^{\gamma_D} f_{\gamma_{SR}} d\gamma_{SR} - \int_0^{\gamma_{SD}} f_{\gamma_{SR}} d\gamma_{SR}$. Thus

$$\begin{aligned} p_1 &= \int_0^{\infty}\int_0^{\gamma_D}\int_{2^{-2R_S}(1+\gamma_{SR})-1}^{\infty} g_{\gamma_D} f_{\gamma_{SR}} g_{\gamma_E} d\gamma_E d\gamma_{SR} d\gamma_D \\ &\quad - \int_0^{\infty}\int_0^{\gamma_{SD}}\int_{2^{-2R_S}(1+\gamma_{SR})-1}^{\infty} g_{\gamma_{SD}} f_{\gamma_{SR}} g_{\gamma_E} d\gamma_E d\gamma_{SR} d\gamma_{SD} \end{aligned} \tag{11}$$

Similarly, p_2 is derevid as shown in (12). It is worth noting that both intersections, $\gamma_{SR} > \gamma_{SD}$ and $\gamma_{SR} \geq \gamma_D$, are not to be considered, for the sake of the fact that last intersection contains the first area.

$$p_2 = \int_0^{\infty}\int_{\gamma_D}^{\infty}\int_{2^{-2R_S}(1+\gamma_D)-1}^{\infty} g_{\gamma_D} f_{\gamma_{SR}} g_{\gamma_E} d\gamma_E d\gamma_{SR} d\gamma_D \tag{12}$$

From what has been discussed above, by combining the results of (11) and (12) and substituting back into (10), the SOP of the cooperative phase is obtained as

$$p_{coop} = \frac{2^{4R_S}\overline{\gamma_{SR}}\left(\overline{\gamma_{RD}} + \overline{\gamma_{SR}}\right)}{\overline{\gamma_{RE}} - \overline{\gamma_{SE}}}\left[A\left(\overline{\gamma_{RE}}\right) - A\left(\overline{\gamma_{SE}}\right)\right] \tag{13}$$

where $A(x) = e^{(1-2^{-2R_S})/x}x^3[\overline{\gamma_{SR}}\,\overline{\gamma_{RD}} + 2^{2R_S}x(\overline{\gamma_{SR}} + \overline{\gamma_{RD}})]^{-1}/(\overline{\gamma_{SR}}\,\overline{\gamma_{SD}} + 2^{2R_S}x(\overline{\gamma_{SR}} + \overline{\gamma_{SD}}))$.

Finally, the overall SOP of EET is derived after plugging (9) and (13) in (7).

3.1.2. Derivation for DT. In the direct transmission scheme, the sensor S always sends collected data to intended controller D according to a transmit rate R_S in the two phases, while the relay remains silent. Then we can obtain an exact expression for the SOP of DT in the following theorem.

Theorem 1.

$$P_{out}^{DT} = 1 - \frac{\overline{\gamma_{SD}}}{\overline{\gamma_{SD}} + 2^{2R_S}\overline{\gamma_{SE}}}\exp\left(\frac{1-2^{2R_S}}{2\overline{\gamma_{SD}}}\right) \tag{14}$$

Proof. See the appendix. □

3.1.3. Derivation for DF. Notably, different from EET, the relay R is always active in DF. The capacity of the main channel $C_L^{DF} = (1/2)\min[\log_2(1+\gamma_{SR}), \log_2(1+\gamma_{SD}+\gamma_{RD})]$, which obviously indicates a performance deficiency, as the transmission rate must meet the requirements of the S-R link. The SOP of DF can be formulated as [21]

$$\begin{aligned} P_{out}^{DF} &= \Pr\left\{\frac{1+\min\left(\gamma_{SR},\gamma_D\right)}{1+\gamma_E} < 2^{2R_S}\right\} \\ &= \frac{B\left(\overline{\gamma_{SR}},\overline{\gamma_{RE}}\right) - B\left(\overline{\gamma_{SR}},\overline{\gamma_{SE}}\right)}{\overline{\gamma_{RE}} - \overline{\gamma_{SE}}} \\ &\quad + \frac{\overline{\gamma_{SR}}B\left(\overline{\gamma_{SR}},\overline{\gamma_{SE}}\right)\left[D\left(\overline{\gamma_{SE}},\overline{\gamma_{SD}}\right) - D\left(\overline{\gamma_{SE}},\overline{\gamma_{RD}}\right)\right]}{2^{2R_S}\left(\overline{\gamma_{RE}} - \overline{\gamma_{SE}}\right)\left(\overline{\gamma_{RD}} - \overline{\gamma_{SD}}\right)} \\ &\quad - \frac{\overline{\gamma_{SR}}B\left(\overline{\gamma_{SR}},\overline{\gamma_{RE}}\right)\left[D\left(\overline{\gamma_{RE}},\overline{\gamma_{SD}}\right) - D\left(\overline{\gamma_{RE}},\overline{\gamma_{RD}}\right)\right]}{2^{2R_S}\left(\overline{\gamma_{RE}} - \overline{\gamma_{SE}}\right)\left(\overline{\gamma_{RD}} - \overline{\gamma_{SD}}\right)} \end{aligned} \tag{15}$$

where $B(x,y) \triangleq (y^2/(x2^{-2R_S}+y))\exp((1-2^{-2R_S})/y)$ and $D(x,y) \triangleq y\overline{\gamma_{SR}}/(x(y+\overline{\gamma_{SR}}) + y\overline{\gamma_{SR}}2^{-2R_S})$.

3.1.4. Derivation for AF. For AF scheme, similar to DF, the relay completes a total transmission in two stages; that is, the source broadcasts the signal, which is then amplified and transmitted to D by the relay R with a variable gain. The SOP of the AF scheme as found in [22] is reproduced as

$$\begin{aligned} P_{out}^{AF} &= \Pr\left\{\log_2\left(\frac{1+\gamma_{SD}+\gamma_{SR}\gamma_{RD}/\left(1+\gamma_{SR}+\gamma_{RD}\right)}{1+\gamma_{SE}+\gamma_{SR}\gamma_{RE}/\left(1+\gamma_{SR}+\gamma_{RE}\right)}\right)\right. \\ &\quad \left. < 2R_S\right\} \approx \frac{\overline{\gamma_D}\left[B\left(\overline{\gamma_D},\overline{\gamma_E}\right) - B\left(\overline{\gamma_D},\overline{\gamma_{SE}}\right)\right]}{\left(\overline{\gamma_E} - \overline{\gamma_{SE}}\right)\left(\overline{\gamma_D} - \overline{\gamma_{SD}}\right)} \\ &\quad - \frac{\overline{\gamma_{SD}}\left[B\left(\overline{\gamma_{SD}},\overline{\gamma_E}\right) - B\left(\overline{\gamma_{SD}},\overline{\gamma_{SE}}\right)\right]}{\left(\overline{\gamma_E} - \overline{\gamma_{SE}}\right)\left(\overline{\gamma_D} - \overline{\gamma_{SD}}\right)} \end{aligned} \tag{16}$$

3.1.5. Derivation for CJ. CJ can be adopted to interfere E by resorting to the relay to transmit interference signal, in which jamming is utilized in a cooperative manner to provide a secure communication link between the sensor and the desired controller to improve the secrecy performance of IoT uplink transmission. Thus, the SOP of CJ can be derived as [21]

$$\begin{aligned} P_{out}^{CJ} &= \Pr\left\{\log_2\left(\frac{1+\gamma_{SD}/\left(1+\gamma_{RD}\right)}{1+\gamma_{SE}/\left(1+\gamma_{RE}\right)}\right) < R_S\right\} \\ &= 1 + \frac{\exp\left(-c\right)}{\overline{\gamma_{RE}}\,\overline{\gamma_{RD}}l}\left(\frac{1}{g} - \frac{1}{h\lg^2}\right)F\left(g+gh\right) \\ &\quad + \frac{\exp\left(-c\right)}{\overline{\gamma_{RE}}\,\overline{\gamma_{RD}}l}\left[\left(\frac{1}{h\lg^2} + \frac{1}{hg}\right)F\left(\frac{1+h}{h\overline{\gamma_{RE}}}\right) - \frac{\overline{\gamma_{RE}}}{g}\right] \end{aligned} \tag{17}$$

where $c \triangleq (2^{R_S}-1)/\overline{\gamma_{SD}}$, $g \triangleq (1+\overline{\gamma_{RD}}c)/\overline{\gamma_{RD}}$, $h \triangleq \overline{\gamma_{SD}}/\overline{\gamma_{SE}}(1+\overline{\gamma_{SD}}c)$, $l \triangleq 1 - 1/\overline{\gamma_{RE}}gh$, $F(x) \triangleq \exp(x)E(x)$, and $E(x) \triangleq \int_x^\infty(\exp(-t)/t)dt$.

3.2. Secure Energy Efficiency. Actually, improvements of security often come at the cost of higher power. In consideration of sustainability, excessive pursuit of security performance is detrimental to IoT devices. In terms of IoT applications, secrecy communications should be conducted in an energy-efficient manner. Consequently, the SEE is used here as the best metric to measure physical layer security and energy efficiency at the same time. Mathematically, the SEE is expressed as

$$\eta_S = \frac{R_S\left(1 - P_{out}^{sch}\right)}{P_{total}^{sch}} \tag{18}$$

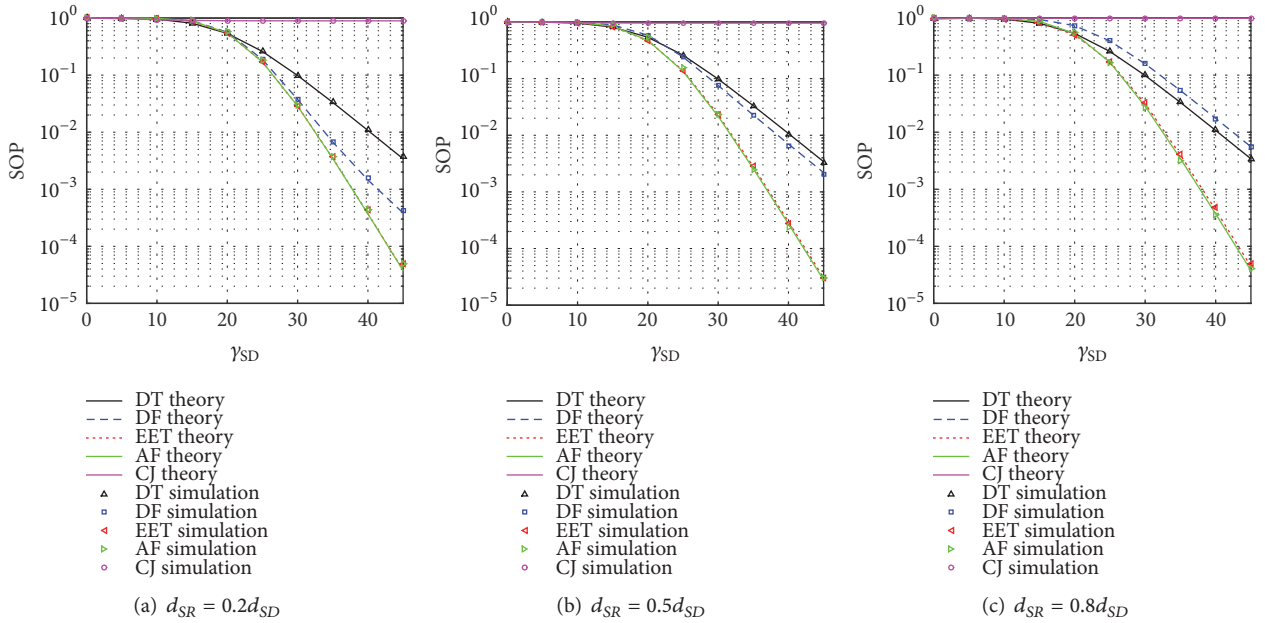
where P_{total}^{sch} denotes the total power consumption of each transmission strategy; that is, $sch \in$ EET, DT, DF, AF, and CJ, which are derived as

$$\begin{aligned} P_{total}^{EET} &= \left(2P_S + 2P_{TX} + 2P_{RX}\right)\Pr\left\{\gamma_{SD} \geq \gamma_{SR}\right\} \\ &\quad + \left(P_S + P_R + 2P_{TX} + 3P_{RX}\right)\Pr\left\{\gamma_{SD} < \gamma_{SR}\right\} \end{aligned} \tag{19}$$

$$P_{total}^{DT} = 2P_S + 2P_{TX} + 2P_{RX} \tag{20}$$

$$P_{total}^{DF} = P_{total}^{AF} = P_S + P_R + 2P_{TX} + 3P_{RX} \tag{21}$$

$$P_{total}^{CJ} = P_S + P_R + 2P_{TX} + P_{RX} \tag{22}$$



(a) $d_{SR} = 0.2d_{SD}$ (b) $d_{SR} = 0.5d_{SD}$ (c) $d_{SR} = 0.8d_{SD}$

FIGURE 2: Secrecy outage probability versus γ_{SD} for different positions of the relay.

where P_{TX} and P_{RX} denote the power costed by the transmit and receive circuitry, respectively. P_S and P_R represent the power spent by the sensor source and by the relay. For simplicity, we assume that $P_S = P_R = P$ in this paper. Furthermore, it is worth noting that the power consumption at E is neglected. Obviously, the denominator of SEE is an increasing function for sending power. Thus, increasement of the power will cause SEE to drop. Note that SEE works as a convex function of the targeted rate. Therefore, we illustrate the optimization problem as

$$\max_{R_S,P} \eta_S \tag{23}$$

It is obviously seen that the exact optimal expressions of R_S and P are very difficult to derive. However, we can use simulation and numerical evaluation to obtain the desired R_S and P via searching algorithm. It should be emphasized that the above expression in (23) has more pragmatic significance for IoT.

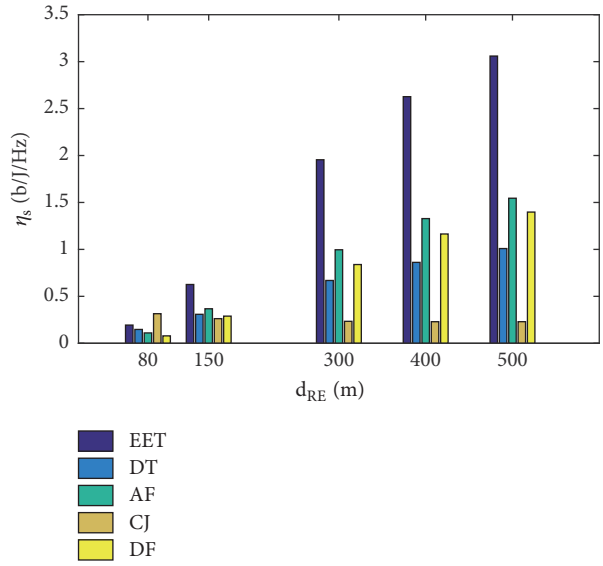


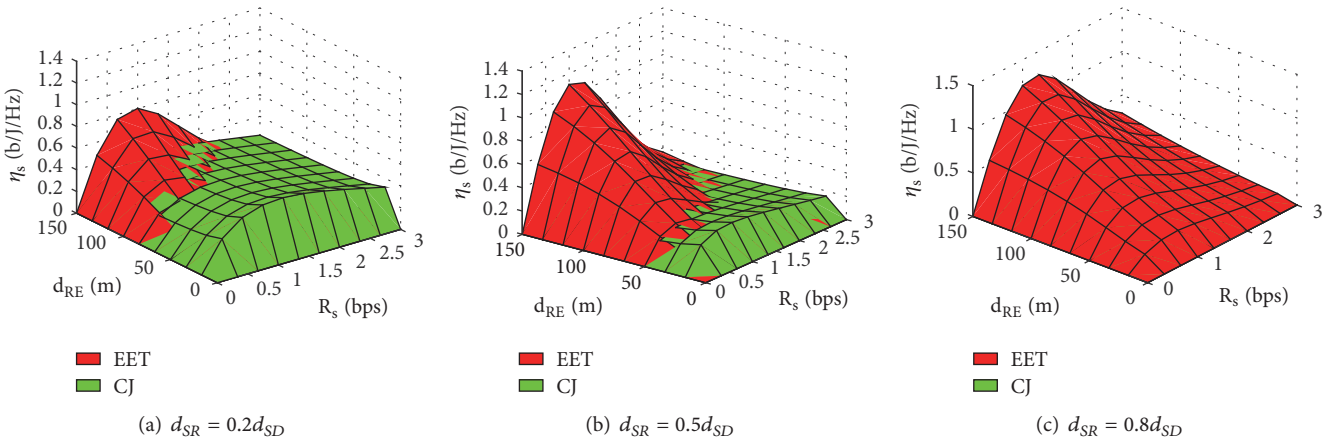
FIGURE 3: Secure energy efficiency versus d_{RE}.

4. Numerical Results

This section provides some numerical simulations to prove the previous theoretical analysis. The parameter configurations in the simulation are set as follows: R_S = 2bps/Hz, d_{SD} = 100m, υ = 2, P_{TX} = 112.2mW, P_{RX} = 97.9mW, B = 10kHz, N_0 = -174dBm/Hz, a link margin of M_l = 10dB, antenna gain G = 5dBi, noise N_f = 10dB, and f = 2.5GHz.

Figures 2(a), 2(b), and 2(c) show the impact of γ_{SD} on the SOP of EET, DT, DF, AF, and CJ transmission strategies for different positions of the relay, respectively, where we observe that, except CJ, the SOP of different transmission strategies was improved by increasing γ_{SD}. This is because increasing the transmitting power benefits both the legitimate destination and cooperative relay. Additionally, it is clearly seen that the simulation results and the theoretical curve match exactly in the whole region, which verifies the accuracy of our conclusions. On the other hand, although the location of the relay changes constantly, the proposed EET and AF can always achieve almost the same optimal secrecy performance. In fact, AF outperforms conventional cooperative schemes (i.e., DF and CJ) in terms of SOP; only if E is closer to relay, CJ has better performance than AF [21]; then we can conclude that the designed EET is a secure cooperative transmission strategy.

When the distance between relay R and E changes, Figure 3 compares the maximum SEE of EET, DT, DF, AF,



(a) $d_{SR} = 0.2d_{SD}$ (b) $d_{SR} = 0.5d_{SD}$ (c) $d_{SR} = 0.8d_{SD}$

FIGURE 4: Secure energy efficiency of EET and CJ versus R_S and d_{RE} for different positions of the relay.

and CJ with the assist of searching methods, which can be used to find the optimal R_S and transmit power. We observe that when E is closer to the legal node, CJ can obtain the best efficiency. On the other hand, when E is far from the legal node, EET performs better in energy efficiency, which confirms that the designed EET is a more energy-efficient secure transmission strategy. Therefore, EET is a low-power green transmission protocol to improve unit energy efficiency for the IoT communication.

In Figure 4, we compare the performance at different transmission rates and at different distances between E and the relay R. For ease of analysis, we just provide the performance comparison between EET and CJ. As the figures show, it is obvious that the performance of the strategies relies on both d_{RE} and R_S. Meanwhile, it is clearly seen that the transmission rate produces a greater impact on EET, and its performance is better when the rate is appropriately low. Thereby, when the EET strategy is adopted in the IoT uplink transmission, for the sake of improving the secrecy performance and energy efficiency of communication systems, a much lower R_S is more suitable. In addition, the location of the relay also has some effects on the EET scheme. Figure 4(a) describes that if the sensor S is closer to the relay R and E stays away from R, EET performs better in contrast to the scenario where E is closer to R. However, if the relay R is closer to the controller D, as shown in Figure 4(c), the jamming signal sent by the relay R will cause serious impact on D, which makes SEE of proposed EET better than CJ. Therefore, we conclude that a more effective energy-efficient secure transmission is introduced by the EET scheme.

5. Conclusion

Secure energy efficiency and physical layer security were investigated in the secure uplink transmission scenario for IoT applications in this paper. Utilizing the advantages of direct and relay links, we proposed a novel energy-efficient secure transmission strategy based on the CSI of the legitimate link (EET), by which the best path is decided between direct and cooperative transmissions, to deal with implementation limits of the IoT devices. The closed-form expressions of SOP and SEE of EET were also derived. In order to show the effectiveness of our new strategy, we further compared the secrecy performance of different transmission schemes such as DF, AF, and CJ as well as DT. The simulation results demonstrated that the proposed EET outperforms other protocols in terms of SEE in most situations. To further enhance the secrecy performance of the IoT networks, EET can be adopted as an effective additional strategy in practical applications. For future work, one interesting aspect is to design the energy-efficient transmission scheme toward secure cooperative IoT in the presence of the multiple eavesdroppers. Other extensions can address another practical issue such as studying the untrusted relays case.

Appendix

By using the formula of full probability, the SOP of DT (14) can be formulated as

$$\begin{aligned} P_{out}^{DT} &= \Pr\left\{C_L^{DT} - C_E^{DT} < R_S\right\} = \Pr\left\{\gamma_{SD} < \nabla\right\} \\ &= \overbrace{\Pr\left\{\gamma_{SD} < \nabla \mid \gamma_{SD} > \gamma_{SE}\right\}}^{\phi_1} \overbrace{\Pr\left\{\gamma_{SD} > \gamma_{SE}\right\}}^{\phi_2} \\ &\quad + \underbrace{\Pr\left\{\gamma_{SD} < \nabla \mid \gamma_{SD} < \gamma_{SE}\right\}}_{\phi_3} \underbrace{\Pr\left\{\gamma_{SD} < \gamma_{SE}\right\}}_{\phi_4} \end{aligned} \tag{A.1}$$

where $\nabla = 2^{2R_S - 1}(1 + 2\gamma_{SE}) - 1/2$. Thus ϕ_2 can be solved as follows:

$$\begin{aligned} \phi_2 &= \Pr\left\{\gamma_{SD} > \gamma_{SE}\right\} = \int_0^{\infty} f_{\gamma_{SD}} d\gamma_{SD} \int_0^{\gamma_{SD}} f_{\gamma_{SE}} d_{\gamma_{SE}} \\ &= \frac{\overline{\gamma_{SD}}}{\overline{\gamma_{SD}} + \overline{\gamma_{SE}}} \end{aligned} \tag{A.2}$$

Similarly, ϕ_4 can be expressed as

$$\phi_4 = \Pr\left\{\gamma_{SD} < \gamma_{SE}\right\} = 1 - \phi_2 = \frac{\overline{\gamma_{SE}}}{\overline{\gamma_{SD}} + \overline{\gamma_{SE}}} \tag{A.3}$$

and ϕ_1 can be obtained as

$$\begin{aligned}\phi_1 &= \Pr\{\gamma_{SD} < \nabla \mid \gamma_{SD} > \gamma_{SE}\} \\ &= \frac{1}{\Pr\{\gamma_{SD} > \gamma_{SE}\}} \int_0^{\infty} f_{\gamma_{SE}} d\gamma_{SE} \overbrace{\int_{\gamma_{SE}}^{\nabla} f_{\gamma_{SD}} d\gamma_{SD}}^{\phi_5}\end{aligned} \tag{A.4}$$

After some simple mathematical manipulations, ϕ_5 in (A.4) can be directly derived as

$$\begin{aligned}\phi_5 = &\exp\left(-\frac{1}{\overline{\gamma_{SD}}}\gamma_{SE}\right) \\ &- \exp\left(\frac{1-2^{2R_S}}{\overline{2\gamma_{SD}}}\right)\exp\left(-\frac{2^{2R_S}}{\overline{\gamma_{SD}}}\gamma_{SE}\right)\end{aligned} \tag{A.5}$$

Therefore, ϕ_1 given by (A.4) can be rewritten as

$$\begin{aligned}\phi_1 &= \frac{\overline{\gamma_{SD}} + \overline{\gamma_{SE}}}{\overline{\gamma_{SD}}} \frac{1}{\overline{\gamma_{SE}}} \int_0^{\infty} \exp\left(-\frac{\gamma_{SE}}{\overline{\gamma_{SE}}}\right) \phi_5 d\gamma_{SE} \\ &= 1 - \frac{\overline{\gamma_{SD}} + \overline{\gamma_{SE}}}{\overline{\gamma_{SD}} + 2^{2R_S}\overline{\gamma_{SE}}} \exp\left(\frac{1-2^{2R_S}}{2\overline{\gamma_{SD}}}\right)\end{aligned} \tag{A.6}$$

Note that when $\gamma_{SD} < \gamma_{SE}$, $C_S = 0 < R_S$; then ϕ_3 can be solved as

$$\phi_3 = \Pr\{\gamma_{SD} < \nabla \mid \gamma_{SD} < \gamma_{SE}\} = 1 \tag{A.7}$$

Finally, the desired expression in (14) can be achieved by summarizing results of (A.2), (A.3), (A.6), and (A.7).

Data Availability

The data in this paper is generated from the simulation in Matlab, and the detail simulation settings can refer to Section 5. Therefore, the data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61501508 and Grant 61671476.

References

[1] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2017.

[2] V. N. Vo, T. G. Nguyen, C. So-In, and D. Ha, "Secrecy Performance Analysis of Energy Harvesting Wireless Sensor Networks With a Friendly Jammer," *IEEE Access*, vol. 5, pp. 25196–25206, 2017.

[3] A. Mukherjee, "Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.

[4] S. Cho, B. F. Spencer, H. Jo et al., "Bridge monitoring using wireless smart sensors," *SPIE Newsroom*, pp. 1–3, 2011.

[5] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.

[6] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, 2016.

[7] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[8] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[9] P. Mu, X. Hu, B. Wang, and Z. Li, "Secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers under secrecy outage probability constraint," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2174–2177, 2015.

[10] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," in *Proceedings of the ICC 2016 - 2016 IEEE International Conference on Communications*, pp. 1–5, Kuala Lumpur, Malaysia, May 2016.

[11] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, Cambridge, UK, 2011.

[12] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[13] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[14] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4985–4997, 2011.

[15] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 359–368, 2012.

[16] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage Constrained Secrecy Throughput Maximization for DF Relay Networks," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1741–1755, 2015.

[17] J. Farhat, G. Brante, and R. D. Souza, "On the Secure Energy Efficiency of TAS/MRC with Relaying and Jamming Strategies," *IEEE Signal Processing Letters*, vol. 24, no. 8, pp. 1228–1232, 2017.

[18] H. Khodakarami and F. Lahouti, "Link adaptation with untrusted relay assignment: Design and performance analysis," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 4874–4883, 2013.

[19] M. Ju, D.-H. Kim, and K.-S. Hwang, "Opportunistic transmission of nonregenerative network with untrusted relay," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 6, pp. 2703–2709, 2015.

[20] J.-B. Kim, J. Lim, and J. M. Cioffi, "Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3866–3876, 2015.

[21] F. Gabry, R. Thobaben, and M. Skoglund, "Outage performances for amplify-and-forward, decode-and-forward and cooperative jamming strategies for the wiretap channel," in *Proceedings of the 2011 IEEE Wireless Communications and Networking Conference, WCNC 2011*, pp. 1328–1333, Mexico, March 2011.

[22] F. Gabry, S. Salimi, R. Thobaben, and M. Skoglund, "High SNR performance of amplify-and-forward relaying in Rayleigh fading wiretap channels," in *Proceedings of the 2013 Iran Workshop on Communication and Information Theory, IWCIT 2013*, pp. 1–5, Iran, May 2013.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 3078272, 18 pages
https://doi.org/10.1155/2018/3078272

Research Article

SCCAF: A Secure and Compliant Continuous Assessment Framework in Cloud-Based IoT Context

Xiang Li,[1] Xin Jin,[1] Qixu Wang,[2] Mingsheng Cao,[3] and Xingshu Chen[2]

[1]*College of Computer Science/Cybersecurity Research Institute, Sichuan University, Chengdu, Sichuan Province 610065, China*
[2]*College of Cybersecurity/Cybersecurity Research Institute, Sichuan University, Chengdu, Sichuan Province 610065, China*
[3]*School of Information and Software Engineering, University of Electronic Science and Technology of China, ChengDu, China*

Correspondence should be addressed to Xingshu Chen; chenxsh@scu.edu.cn

Received 22 June 2018; Accepted 27 September 2018; Published 23 October 2018

Guest Editor: Zhiqing Wei

The Internet of Things (IoT) offers a wide variety of benefits to our daily lives in many ways, ranging from smart wearable devices to industrial systems. However, it also brings well-known security and compliance concerns, especially in the physical layer. In addition, due to numerous IoT architectures which have been developed and deployed based on the cloud, the security and compliance of IoT depend on the cloud thoroughly. In this paper, a secure and compliant continuous assessment framework (SCCAF) is proposed to evaluate the security and compliance levels of cloud services in life-cycle. The SCCAF facilitates cloud service to customers to select an optimal cloud service provider (CSP) which satisfies their desired security requirements. Moreover, it also enables cloud service customers to evaluate the compliance of the selected CSP in the process of using cloud services. To evaluate the performance and availability of SCCAF, we carry out a series of experiments with case study and real-world scenario datasets. Experimental results show that SCCAF can assess the security and compliance of CSPs efficiently and effectively.

1. Introduction

The rise of IoT has led to the constant universal connection between people and things (e.g., sensors or mobile devices), and it plays a remarkable role in all aspects of our daily lives [1, 2]. Furthermore, combined with preeminent technologies such as cloud, the cloud-based IoT architecture is becoming a trend in the IoT market. However, as with many new technologies, there are several challenges when it comes to achieving success in cloud-based IoT context adoption [3–5]. Two of the biggest concerns for cloud-based IoT context are security (especially, the physical layer security) and compliance (e.g., lack of customer control mechanism, security assurance and service level agreements (SLAs) guarantee, and dynamic change in the IoT devices) [6, 7]. Nevertheless, there is little literature on the IoT security and compliance assessment [8]. The traditional existing literatures with respect to security of IoT focus on dealing with wireless networks [2, 9, 10]. Therefore, the premise of securing the cloud-based IoT context is to evaluate the security and compliance of cloud service.

Due to massive number of CSPs offering similar kinds of services in the cloud market, it becomes a tricky challenge to select an optimal cloud service. Moreover, from the perspective of cloud service customers (CSCs), it is becoming more and more important to identify which is the real optimal cloud service provider (CSP). A real optimal CSP is supposed to satisfy the security requirements of CSCs in the process of deploying cloud service and the compliance requirements of SLAs continuously while the cloud service is operating. Before CSCs are planning to use cloud services, the major challenge is to select a security CSP among various CSPs based on their security requirements. After that, the main challenge for CSCs is to ensure the conformance between the actual quality of service (QoS) of cloud services and the SLAs claimed by the selected CSP. Intuitively, security and compliance issues are equally important to CSCs throughout the entire process of using the cloud service.

However, the actual situation is that CSCs frequently concentrate on the security or compliance in different periods of using cloud service. Security is the primary concern for CSCs while selecting CSP and the main obstacle of promoting

cloud computing. Nonetheless, research results usually target selecting the security CSP and overlook the compliance issue [11–16]. On the other hand, compliance is the critical concern for CSCs while using cloud services. But the significance of security and the feasibility of assessment tend to be ignored [17–19]. For instance, it is almost impossible for CSCs to evaluate trustworthiness of cloud services by objective and direct means (e.g., QoS monitoring). It is due to the fact that before signing a service contract with CSC, CSP will neither provide the technical details of cloud services nor open interface to CSCs to monitor service QoS for the purpose of confidentiality, security, and competition.

As aforementioned, few literatures take the integration of security and compliance assessment into consideration for evaluating the cloud service. To the best of our knowledge, there is no continuous assessment framework existing in literature which concatenates security and compliance of cloud service from comprehensive perspective. Moreover, the compliance issues of cloud service are urgent and worth studying, especially during the use of cloud services.

In this paper, we propose a novel secure and compliant continuous assessment framework (SCCAF), which evaluates the security level and the compliance level of cloud service. Additionally, a new concept of cloud service life-cycle (CSL) is proposed and elaborated. The CSL enables CSCs to well understand the objects which need to be considered for adopting cloud services. Accordingly, SCCAF can offer more flexibility in the hands of CSCs to evaluate cloud on the basis of their security and compliance requirements.

In a nutshell, the main contributions in this paper are summarized as follows.

(i) We propose a new concept of cloud service life-cycle which enables CSCs to well understand the objectives that need to be considered at each phase of the adoption of cloud services.

(ii) The SCCAF, a novel secure and compliant continuous assessment framework based on CSL, is proposed. It combines assessment methods of security and compliance as mutual complementation. Hence, the SCCAF enables CSCs to continuously evaluate the cloud service provided by CSPs during the full CSL.

(iii) To illustrate the efficiency and effectiveness, we conduct comprehensive experiments to validate our proposed SCCAF from two dimensions, respectively. The results show that SCCAF can achieve better performance and availability.

The rest of the paper is organized as follows. Section 2 surveys related work. Section 3 introduces the proposed concept of CSL and Section 4 elaborates the SCCAF. Section 5 presents the experimental results and their analyses for validating our proposed assessment method. Section 6 concludes this paper with directions for future work.

2. Related Work

A variety of recent research works target selecting an optimal CSP by evaluating cloud services from the dimensions of security and trust. One example is Luna et al. [20] who presented a security metrics framework for CSPs security assessment. In [21], a methodology to quantitative benchmark CSPs security SLA with respect to the security requirements of CSC is presented based on the reference evaluation methodology [22]. Paper [14] presents a methodology for quantizing and evaluating security threats, which weighs each security threat to consider which security controls are required to meet the users' needs in a security SLA, and in [23] a new technique for conducting quantitative and qualitative analysis of the security level provided by CSPs is proposed. Both works are based on the analytic hierarchy process (AHP) [24]. In [11], two evaluation techniques are proposed to conduct the quantitative assessment and analysis of the security SLA based security level provided by CSPs with respect to a set of CSCs security requirements. In [12], a novel cloud security assessment technique is presented which is a more simple and effective approach that can be deployed for the needed online real-time assessment and offers both accuracy and high computational efficiency. Refernce [13] presents a methodology for evaluation and selection of cloud services based on a multicriteria analysis [25] process using a set of evaluation criteria and quantitative metrics. However, the security assessment methods mentioned above are all about selecting CSP before CSCs use of cloud services, and none of them is involved in the case of, after selecting CSP, how to determine the compliance of the SLA claimed by the CSP in the runtime of cloud service.

Besides the security assessment, the assessment techniques to select CSP have also been focused on the evaluation of trust, which has captured researchers' attention in recent years. The assessment methods based on the trust are mainly divided into two aspects, including subjective assessment and objective assessment. From the subjective perspective, [26] presents a distributed framework for determining trustworthiness of federated cloud entities, which uses a reputation manager to capture and store the behavior of cloud entities. In [27], a trust management model is proposed which comprises SLA agent, cloud service directory, cloud provider, and cloud consumer to select most reliable cloud providers by managing trust relationships based on three types of information (local experience of consumers with providers, opinion of others, and reports provided by SLA agent). Paper [28] proposed a model of reputation-enhanced QoS-based web services discovery that combines an augmented UDDI registry to publish the QoS information and a reputation manager to assign reputation scores to the services based on customer feedback ratings on their performance. In [29], a trust management approach is presented, namely, ServiceTrust, and it takes rater's credibility into consideration by combining a user's needs and other personal ratings to estimate a CSP's trust value for the support of reputation-oriented service selection. However, the subjective assessment methods which are difficult to quantify usually makes the evaluation results less accurate and also presents difficulty in its practical adoption.

Many objective assessment methods of service selection have also been proposed, such as those based on monitored QoS data [30–35]. These works mainly focus on determining

the most satisfactory services according to users' requirements and preferences relative to QoS. However, not all of these works apply to cloud environment. Moreover, QoS data of services is hard to be acquired [36] and might not be reliable [34]. To select a satisfactory CSP from objective perspective, [37] proposed a ranking technique that utilizes performance data to measure various QoS attributes and evaluates the relative ranking of cloud providers. In [38], a QoS ranking prediction framework is presented for cloud services by taking advantage of the past service usage experiences of other consumers, which requires no additional invocations of cloud services. Authors of [39, 40] propose an automated framework called CloudGenius and a comparative framework named CloudCmp, respectively. The purpose of the former is automating the decision-making process based on a model and factors specifically for web server migration to the cloud. The purpose of the latter is measuring the elastic computing, persistent storage, and networking services offered by a cloud along metrics that directly reflect their impact on the performance of customer applications. Both of them provide mechanisms to evaluate performance indicators of CSPs in order to help customers pick a cloud that fits their needs.

In addition, there are a few works combining subjective perception and objective measurement to evaluate trustworthiness of cloud services. Reference [19] designs a novel framework named CSTrust for conducting cloud service trustworthiness evaluation by combining QoS prediction and customer satisfaction estimation. Reference [18] proposes a trustworthy selection framework for cloud service selection named TRUSS, which contains an integrated trust evaluation method via combining objective trust assessment and subjective trust assessment. Paper [41] proposes a novel trust evaluation method named UsageQoS for accurately measuring quality of cloud services via leveraging service QoS parameters and user ratings. Although objective assessment methods can yield more accurate results and are easier to implement through existing technical means, they ignore the fact that security is one of the major barriers for adoption of cloud computing and the paramount consideration for CSCs. Moreover, as stated earlier, CSCs are unable to evaluate trustworthiness of cloud services by objective and direct technical means before selecting a CSP to provide cloud services.

As can be seen from the related work discussed above that many existing literatures evaluate security or trustworthiness of CSPs for merely selecting an optimal CSP, but they overlook an important issue; that is, CSCs are concerned about the compliance of SLAs claimed by CSP during the use of cloud services. However, there is no comprehensive and continuous assessment framework that combines security and compliance as a complete and complementary attribute to facilitate CSCs to continuously evaluate CSPs during the full cloud service life-cycle. This paper presents a concept of cloud service life-cycle (CSL) from CSCs' perspective that enables CSCs to clearly understand the items that need to be considered at each phase of the adoption of cloud services. Then a secure and compliant continuous assessment framework is proposed based on CSL, which concatenates security and compliance assessment methods. Such a framework not only enables CSCs to select a security CSP from numerous candidate CSPs out of security perspective, but also allows CSCs to evaluate the compliance of SLAs claimed by the selected CSP in the cloud service runtime. Compliance assessment result can help CSCs make further decisions (e.g., continue to use, change CSP, seek remedies, and claims and even terminate cloud service).

3. Cloud Service Life-Cycle

In this paper, cloud service life-cycle (CSL) is articulated as an assumption or an expectation that a CSC will experience a continuous and integral process about adopting cloud service. This assumption or expectation is based upon a series of more specific phases, which form the components of CSL. As shown in Figure 1, the CSL, an extension from our previous work [43], comprises six phases: initial preparation, alternatives choice, solution deployment, continuous monitoring, decision making, and termination of service. The detailed phases of CLS are described as bellow.

(1) Initial Preparation. Initial preparation is the first phase for all the potential CSCs that are eager to leverage the benefits of cloud services. Customers should analyze the benefits of using cloud computing services based on their data and business types and determine whether the cloud computing services are suitable for them. At the same time, they should determine cloud capabilities types and cloud service categories in accordance with their data and business characteristics. As mentioned above, security is the top primary concern for customers to adopt cloud services. Therefore, CSC should conduct security demand analysis according to the key characteristics and potential security threats of cloud computing. Additionally, the main objective of this phase is that CSC defines the security metrics in accordance with the security analysis results for the preparation of selecting the optimal CSP in next phase.

(2) Alternative Selection. In the alternative selection phase, CSC should select an appropriate CSP in accordance with their security requirements and the security capability of cloud services. Due to the competition among various CSPs, there is large number of CSPs offering similar kinds of cloud services and security provisions. As a result, it has become a challenging task for CSC to identify which service is the best appropriate for them. Hence, to ensure data and business security, CSC should take advantage of the security metrics defined in the previous phase. At the same time, CSC can employ an effective security assessment method to evaluate the security level of CSPs. Customers can select the optimal CSP to provide cloud service based on the security assessment result. The security assessment method involved in this phase is the focus of this paper, which will be elaborated later.

(3) Solution Deployment. In order to ensure robust and efficient use of cloud services, the primary purpose for CSC is to negotiate with the selected optimal CSP to set up the cloud SLAs, which stipulates the QoS of cloud services offered

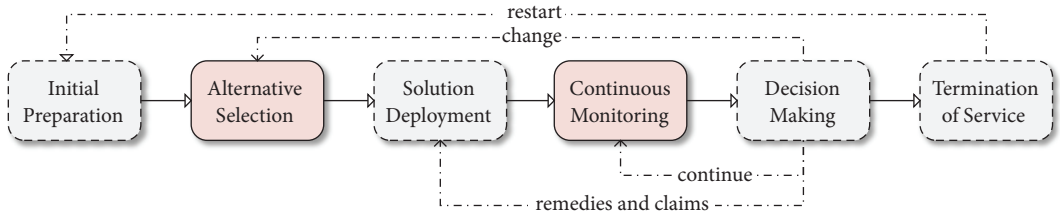


Figure 1: Cloud service life-cycle.

by the CSP. In the meanwhile, CSC should also negotiate with the CSP on the terms including the remedies and claims and change service provider and termination of service in case that the CSP violates the agreed QoS in the operational process of cloud services. Therefore, CSC should define compliance metrics based on the analysis of actual business requirements and the agreed SLAs, which will be used for compliance evaluation of cloud services in the next phase. Finally, CSC should confirm the deployment plan developed by the selected CSP and entrust the CSP to deploy cloud service.

(4) Continuous Monitoring. The primary purpose of CSC in the phase of continuous monitoring is to ensure that actual QoS in the runtime of the cloud service conforms with the QoS agreed in SLAs. In light of planned and unplanned changes that occur in the cloud environment over time, the state of cloud services is not always maintained. Moreover, the CSP may be likely to achieve the benefit maximization at the expense of service quality; that is, CSP not always fully comply with the QoS in the SLAs to offer cloud services, especially that the CSC are not aware of SLAs while the CSP may reduce cloud computing resources (e.g., computing, storage, and network). Therefore, CSC should continuously monitor and record cloud service quality in the process of using cloud services and evaluate the conformance of cloud services through an effective compliance assessment method. The compliance assessment method involved in this phase is the focus of this paper, which will be elaborated later.

(5) Decision Making. In this phase, compliance assessment results in the previous phase can help CSC make decisions. CSC can determine which measures will be taken according to their tolerance to the compliance level of cloud services, which have an impact on their business performance (e.g., reliability and availability). In other words, the CSCs can decide to take corresponding measures according to the violation extent of SLAs. For example, if cloud services are compliant, namely, the monitoring QoS of cloud services is complying with the agreed QoS of SLAs, CSCs can decide to continue to use and evaluate the cloud services. If the cloud services are not compliant, CSC can decide to change CSP or seek remedies and claims to the CSP according to the violation extent, as shown in Figure 1. In the worst case, CSC can choose to terminate the cloud service and exit. The establishment of compliance rules and corresponding measures will be elaborated later.

(6) Termination of Service. The termination of cloud service deals with the exit process, where the use of a cloud service is terminated. Once CSC choose to exit the cloud service, they need to focus on addressing specific termination issues including the exit process and the handling of all classes of data related to the cloud service. For instance, the CSC is able to retrieve their cloud service data and application artifacts. In the meantime, the CSP needs to delete all the CSCs' data. Moreover, the CSC expects that the CSP will not retain any materials belonging to CSC after an agreed period. After exiting cloud service, CSCs can repeat the "Initial Preparation" phase when considering using cloud service again. At the end of the exit process, the CSP should provide the CSC with notification that the process is complete.

4. The Proposed Framework

In this section, the SCCAF, a CSL-based continuous assessment framework, is proposed. This framework can be divided into three main processes, encompassing (1) security assessment, (2) compliance assessment, and (3) taking measures. As shown in Figure 2, the SCCAF includes the following steps.

(1) *Security Assessment*. The CSC evaluates the security level of alternatives (CSPs) according to the conformance between the claimed security provisions provided by CSPs and the security metrics (e.g., facility security, risk management, and information security) defined by the CSC. Then, the CSC selects the optimal CSP to deploy cloud service based on the security assessment result as shown in Figure 3. The security assessment is implemented in initial preparation and alternative selection phases of CSL.

(2) *Compliance Assessment*. After the security assessment is completed, the CSC can select the optimal (high security level) CSP to provide cloud service. During the use of cloud service, the CSC evaluates the compliance level of the cloud services based on the conformance between the claimed cloud SLAs and the actual QoS, as shown in Figure 4. The premise for compliance assessment is that CSC defines the compliance metrics in the solution deployment phase of CSL, namely, specific requirements of SLAs. The compliance assessment is implemented in continuous monitoring phase of CSL.

(3) *Taking Measures*. After the compliance assessment is completed, the CSC can establish compliance

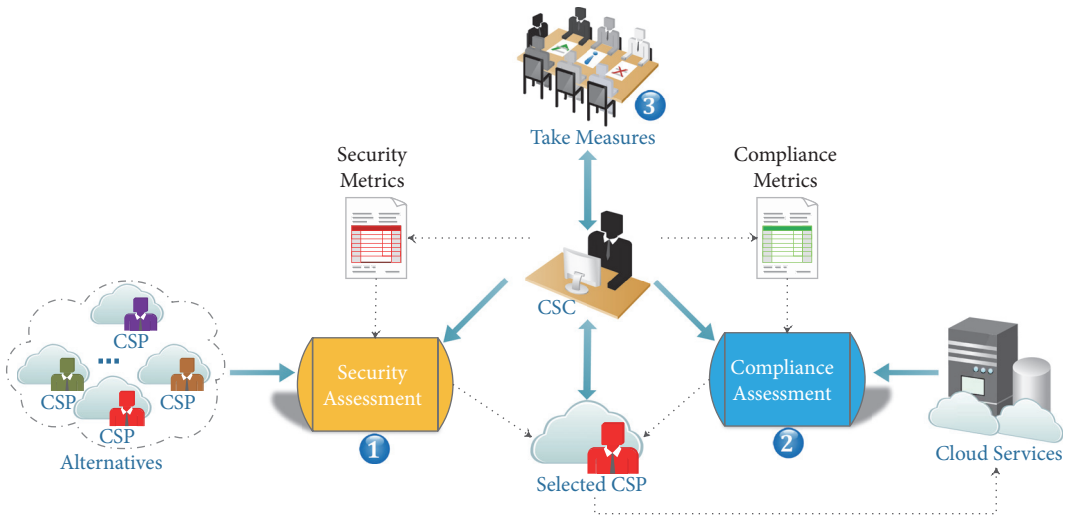


Figure 2: The system architecture of SCCAF.

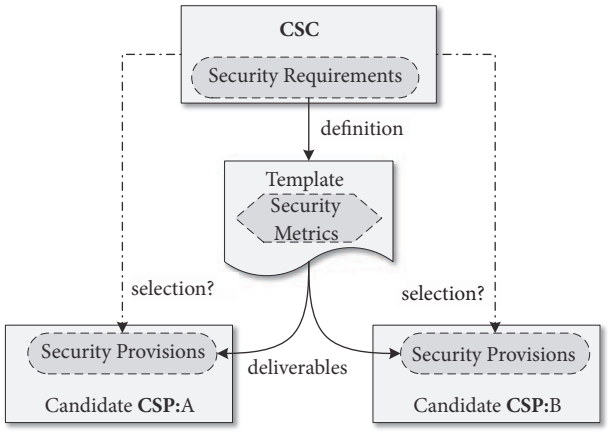


Figure 3: The definition and employment of security metrics.

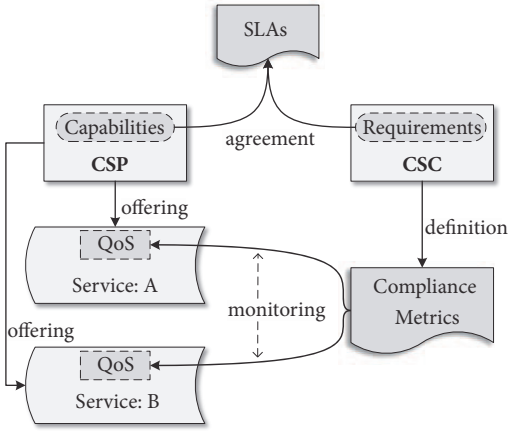


Figure 4: The definition and employment of compliance metrics.

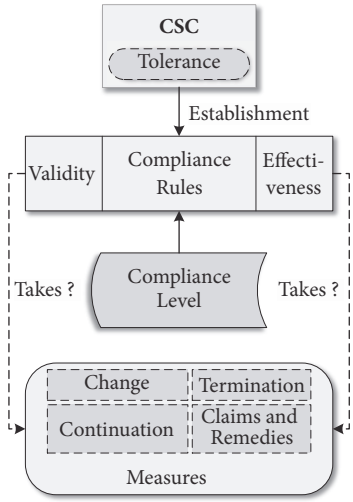


Figure 5: Taking measures according to the compliance level.

tolerance rules based on the impact of compliance level on their actual business. Then, CSC can take corresponding measures (e.g., change CSP, continue to use, and seek remedies and claims) according to the compliance level of the cloud services, as shown in Figure 5. In the worst case, the CSC may consider terminating the cloud service. The process of taking measures is implemented in the decision-making phase of CSL.

4.1. Security Assessment. In security assessment process, the CSC defines security metrics, which include CSC's security requirements related to its data and business. The CSPs determine and describe the conformance between security metrics and their security provisions. According to this conformance, the proposed security assessment approach evaluates the security level of CSPs and ranks them based on the evaluation result. The quantitative security level of CSPs is the primary objective of the security assessment process. For convenience, the key notations used in security assessment are given in Table 1. Specifically, it includes four steps as follows.

(1) Security Metrics Definition. CSC defines a set of security metrics and provides it to CSPs. For instance, CSC can select security controls from the cloud controls matrix (CCM) [44] or consensus assessments initiative questionnaire (CAIQ) [42] according to its security requirements. Then, the CSPs measure their security provisions in accordance with the security metrics and submit measurement results to CSC in the form of deliverables. Deliverables include specific security metrics representing the security provisions of CSPs. The first round using security metrics is to collect information with respect to the security provisions (deliverables) of the CSPs in a uniform format. The deliverables contain n security provisions of m CSPs. The definition of security metrics is implemented in initial preparation phase of CSL.

Table 1: Notations in security assessment.

Symbol	Description
m	the number of CSPs
n	number of security metrics
W_j	weight vector of the pairwise comparison matrix constructed by the *jth* security metric
w	weights assigned to security metrics
K	deliverables set of CSPs
Q_{ij}	quantified security metric in K
$R_{m\times n}$	weighted normalized decision matrix
A^+	ideal solutions of the positive security metric
A^-	ideal solutions of the negative security metric
D_i^+	positive separation measure of the *ith* CSP
D_i^-	positive separation measure of the *ith* CSP
C_i	relative closeness of the *ith* CSP

(2) Security Metrics Quantification. The second round is to quantify the security metrics (deliverables) of each CSP for convenient comparison of their security capabilities. The quantification approach depends on different comparison types of different security metrics. In this step, we can employ the quantification approach proposed by [11, 23]. This approach quantifies security metrics into two categories: Boolean (e.g., a YES/NO measurement result representing the conformable or unconformable to the security metric) and numeric (e.g., a cryptographic key length measurement result representing the extent of conformance to the security metric). The quantitative deliverables are used as input

dataset $Q_{m\times n}$ of security assessment process. The quantification of security metrics is also implemented in initial preparation phase of CSL.

(3) Weights Assignment. After quantifying security metrics, CSC can determine the weights of security metrics by employing the AHP method [24]. In this step, CSC assigns scale of relative importance from 1 to 9 (e.g., such that 9 represents extremely more important and 1 equal importance) for each security metric. These security metrics with specific numerical value can be used to construct a pairwise comparison matrix according to standard AHP method. At the same time, the consistency of this matrix needs to be validated. Then, the weight vector $\boldsymbol{W}$ can be obtained by calculating the eigenvector corresponding to the maximum eigenvalue of the pairwise comparison matrix [45]. The weights of assigning security metrics denoted as $\boldsymbol{w}$ can be obtained by (1), which holds that $\sum \boldsymbol{w} = 1$.

$$\boldsymbol{w} = \left(w_j\right)_{n\times 1} = \frac{W_j}{\sum_{j=1}^{n} W_j} \tag{1}$$

(4) Security Level Evaluation. For the given quantitative security metrics $Q_{m\times n}$ and their weights $\boldsymbol{w}$, CSC can employ the TOPSIS method [46] to evaluate the security level of each CSP and compare their security level in the same context. In this step, a normalized weighted decision matrix needs to be constructed first by (2).

$$R_{m\times n} = \left(\frac{Q_{ij}}{\sqrt{\sum_{i=1}^{m} Q_{ij}^2}} \right)_{m\times n} \times \boldsymbol{w} \tag{2}$$

Then, the ideal solutions A of each security metric can be determined by (3) and (4), which includes positive A^+ and negative A^-.

$$A^+ = \left\{ min\left(r_{ij}\right) \middle| j \in J^- \ or \ max\left(r_{ij}\right) \middle| \ j \in J^+ \right\} \tag{3}$$

$$A^- = \left\{ max\left(r_{ij}\right) \middle| j \in J^- \ or \ min\left(r_{ij}\right) \middle| \ j \in J^+ \right\} \tag{4}$$

where $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, $r_i j \in R$, J^+ represents the security metrics having a positive impact and J^- represents the security metrics having a negative impact.

After that, separation measures D can be calculated by (5) and (6), which represent the geometric distance from alternatives (CSPs) to ideal solutions A. It includes positive D^+ and negative D^-:

$$D_i^+ = \sqrt{\sum_{j=1}^{n} \left(r_{ij} - r_j^+\right)^2} \tag{5}$$

$$D_i^- = \sqrt{\sum_{j=1}^{n} \left(r_{ij} - r_j^-\right)^2} \tag{6}$$

where $i = 1, 2, \ldots, m$, and D_i^+ and D_i^- denote the separation measure from each alternative (CSP) to positive and negative ideal solutions, respectively.

Input: set of deliverables K of alternatives (CSPs), size of the set $m \times n$
1: **Preprocessing:** Initialization and quantifying the deliverables (security metrics) K as Q according to the category of security metrics.
2: **Weight Assignment:** Applying AHP approach to determine the weight vector $\boldsymbol{w}$ for security metrics.
3: **Security level evaluation:** Construct the weighted normalized decision matrix R with the quantitative deliverables Q by TOPSIS method and the obtained weight vector $\boldsymbol{w}$. Calculate the relative closeness (C) for each alternative.

Algorithm 1: Security Assessment.

Next, the relative closeness C representing the degree of conformity between the alternatives (CSP) and the ideal solution can be obtained by (7):

$$C_i = \frac{D_i^-}{D_i^+ + D_i^-} \tag{7}$$

where $i = 1, 2, \ldots, m$ and $0 \le C_i \le 1$. Then, CSC can rank CSPs according to their relative closeness C and select the optimal one with C closest to 1.

To sum up, the security evaluation process is implemented in alternative selection phase of CSL. Algorithm 1 illustrates the security assessment process in the SCCAF. Algorithm 2 demonstrates the procedure of security level evaluation.

After selecting the optimal CSP, the CSC negotiates with the selected optimal CSP on the details of cloud SLAs, namely, specific QoS stipulations. CSC can define compliance metrics in accordance with the agreed SLAs. The compliance metrics should contain the monitorable and measurable QoS attributes belonging to a specific service and their specific compliance values, namely, details of SLAs claimed by the optimal CSP. Such compliance metric can be exploited to evaluate the compliance level of a cloud service during the period of using cloud services, as shown in Figure 4. Actually, since there has been much literature on the establishment of SLAs, CSC can employ existing methods to determine cloud SLAs and define compliance metrics. For instance, the methods proposed by ISO/IEC [47, 48] can be employed to formulate SLAs. The methods proposed by National Institute of Standards and Technology (NIST) [49] and ISO/IEC [50] can be employed to define the compliance metrics. Therefore, the solution deployment phase of CSL is not the focus of this paper.

According to the compliance metrics, the CSC can evaluate the compliance level of the cloud services by employing the compliance assessment method, which we will elaborate its details as follows.

4.2. Compliance Assessment. The compliance assessment process is performed after the security assessment process yields an optimal CSP who will provide cloud service to

Input: set of deliverables K, the number of alternatives (CSPs) m, the number of security metrics n
1: **procedure** SECURITY LEVEL EVALUATION(k, m, n)
2: Create arrays $C_{1\times m}$, $Q_{m\times n} \longleftarrow \emptyset$;
3: Create vector $\boldsymbol{w}$;
4: $index \longleftarrow 0$;
5: The quantized deliverables K is assigned to Q;
6: $\boldsymbol{w} \longleftarrow$ ASSIGNWEIGHTS4METRICS (K, n);
7: $C \longleftarrow$ OBTAIN THE OPTIMAL ALTERNATIVE ($Q, m, n, \boldsymbol{w}$);
8: $index \longleftarrow$ the index of $Max(C)$;
9: **return** *index*;
10: **end procedure**

ALGORITHM 2: Security Level Evaluation.

TABLE 2: Notations in compliance assessment.

Symbol	Description
$T = \{t_1, t_2, \cdots, t_j\}$	a set of compliance evaluation period
$A = \{a_1, a_2, \cdots, a_i\}$	a set of QoS attributes belonged to a service
$C = \{c_1, c_2, \cdots, c_i\}$	a set of compliance metrics values of A
D_{ij}	a set of monitoring data of a_i within t_j
M_{ij}	the mean of D_{ij}
S_{ij}	the variance of D_{ij}
v_{ij}	single conformance of a_{ij}
P_{ij}	the ratio between M_{ij} and the sum including the means of each t_j
H_{ij}	the entropy of a_{ij}
w_{ij}	weight assigned to v_{ij}
f_i	compliance level of a_i
p	monitoring frequency within t_j

the CSC. In the compliance assessment process, CSC continuously evaluates the compliance level of cloud services according to the compliance metrics. Compliance assessment is performed in terms of periods. The quantitative compliance level of cloud services is the primary objective of the compliance assessment process, which can be referred by CSC to make decisions. For convenience, the key notations used in security assessment are given in Table 2.

Specifically, it includes five steps as follows.

(1) Data Collection and Preprocessing. The CSC determines a set of evaluation period T and a monitoring frequency p within each evaluation period t ($t \in T$). For a given evaluation period T, CSC continuously monitor and record the QoS attributes A of a specific service. Then, a monitoring dataset D with respect to A can be obtained. The first round is to collect and preprocess the monitoring dataset of QoS attributes. For convenience, we take a QoS attribute a_i ($a_i \in A$) as an example to describe the compliance assessment process in detail. For a given QoS attribute a_i, its monitoring dataset D_i ($D_i \subset D$) can be obtained from the dataset D. Moreover, for a given evaluation period t_j, the dataset D_i can be divided into smaller datasets D_{ij} ($D_{ij} \subset D_i$) based on t_j. The datasets D_{ij} are used as input data of compliance assessment process to calculate the single conformance v_{ij} of a_i in each t_j. The compliance level of a_i can be obtained by aggregating the weighted v_{ij} within T.

(2) Compliance Interval Construction. The second round is to construct the compliance interval of a_i in accordance with its monitoring dataset D_{ij}. First, we can calculate the mean M_{ij} and variance S_{ij} of D_{ij} by (8) and (9).

$$M_{ij} = \frac{\sum_{k=1}^{p} D_{ij}^k}{p} \tag{8}$$

$$S_{ij} = \frac{\sum_{k=1}^{p} \left| D_{ij}^k - M_{ij} \right|}{p-1} \tag{9}$$

In fact, the actual monitoring QoS of an attribute fluctuates around the compliance metrics value C of SLAs in the runtime of cloud services (in addition to outage, equipment failure, etc.)[36]. Moreover, its fluctuation range of monitoring data cannot be determined accurately [34]. In addition there are only limited monitoring data for a QoS attribute, namely, a small sample. Therefore, we assume that the variation of monitoring data conform to t-distribution [51]. Then, the compliance interval can be constructed by (10) and (11):

$$L = M_{ij} - \frac{\sqrt{S}}{\sqrt{p}} t_{\alpha/2}(p-1) \tag{10}$$

$$U = M_{ij} + \frac{\sqrt{S}}{\sqrt{p}} t_{\alpha/2}(p-1) \tag{11}$$

where L and U represents the lower and upper bounds of the compliance interval, respectively. α is the confidence level assigned by the CSC. $t_{\alpha/2}$ can be obtained by look-up table [51].

(3) Single Conformance. The single conformance is the compliance value of a QoS attribute a_i in an evaluation period t_j. The third round is to obtain single conformance v_{ij} of a_i according to its compliance interval L, U and compliance value c_i. Since different attributes may have different ranges and units, we normalize QoS values into a unified range [0, 1]. Then, the single conformance v_{ij} can be calculated by (12) and (13). The single conformance can be divided into two different types: Positive Factor v_{ij}^{+} representing that higher is better (e.g., throughput) and Negative Factor v_{ij}^{-} representing that lower is better (e.g., response time).

$$v_{ij}^{+} = \begin{cases} 1 & c_i \leqslant L \\ \dfrac{U - c_i}{U - L} & L < c_i \leqslant U \\ 0 & c_i > U \end{cases} \tag{12}$$

$$v_{ij}^{-} = \begin{cases} 0 & c_i \leqslant L \\ \dfrac{c_i - L}{U - L} & L < c_i < U \\ 1 & c_i \geqslant U \end{cases} \tag{13}$$

(4) Weights Assignment. After obtaining the single conformance of a_i, its weight w_{ij} can be determined by employing the entropy method [52]. Firstly, the entropy of a_i in t_j can be calculated according to its mean M_{ij} and (14) and (15), which is denoted as H_{ij}. P_{ij} represents the ratio between M_{ij} and the sum including the means of each t_j.

$$P_{ij} = \frac{M_{ij}}{\sum_{j=1}^{|T|} M_{ij}} \tag{14}$$

$$H_{ij} = -\frac{1}{\ln |T|} \sum_{j=1}^{|T|} P_{ij} \ln P_{ij} \tag{15}$$

Then, for the weight of assigning to a_i in t_j denoted as w_{ij}, it can be obtained in accordance with (16), which holds that $\sum_{j=1}^{|T|} w_{ij} = 1$.

$$w_{ij} = \frac{1 - H_{ij}}{|T| - \sum_{j=1}^{|T|} H_{ij}} \tag{16}$$

(5) Compliance Level Evaluation. This round is to calculate the compliance level of a_i in accordance with the obtained weight and single conformance. For the compliance level of a_i, each of the weighted single conformance needs to be aggregated in T. According to (17), the compliance level f_i of a_i can be obtained, which holds that $0 \leq f_i \leq 1$. The closer the compliance level is to 1, the more compliant the evaluated attribute is.

$$f_i = \sum_{j=1}^{|T|} v_{ij} w_{ij} \tag{17}$$

Broadly, the compliance assessment process is implemented in continuous monitoring phase of CSL. Algorithm 3 illustrates the compliance assessment process in the SCCAF. Algorithm 4 demonstrates the procedure of compliance level evaluation.

4.3. Take Measures. The process of taking measures is performed after the compliance assessment process yields assessment results regarding the cloud services. In this process, CSC establishes relevant compliance tolerance rules (e.g., assessment validity) on the basis of compliance assessment results. Additionally, these rules need to be associated with the corresponding measures (e.g., change CSP). Then, CSC can determine which measure to be taken based on the conformity between compliance level and the compliance tolerance rules. The primary objective of this process is to help the CSC stop loss in time in the event of cloud SLAs compliance violations. For convenience, the key notations given in the compliance assessment apply to the process of taking measures. The details of compliance tolerance rules and corresponding measures will be described in the following.

(1) Validity. The CSC can establish a validity indicator to determine whether the compliance assessment is valid. For a given evaluation period T, the compliance assessment of cloud service is performed t $(t \in T)$ times, and each of the single conformance v is different. A compliance assessment which subjects to $v \neq 0$ is considered as a valid assessment. Then, we define assessment validity as follows.

Definition 1. Let μ and φ denote the number of valid assessment and invalid assessment within the evaluation period T, respectively. The validity of compliance assessment denoted as o can be calculated by

$$o = \frac{\mu}{\mu + \varphi} \tag{18}$$

The CSC can establish assessment validity threshold based on their actual business requirements. For instance, we assume that the acceptable assessment validity threshold of the CSC is α. Thus, for a given evaluation period T (e.g., a year), the compliance assessment is performed in terms of t $(t \in T)$ (e.g., a day). If the assessment validity o is less than α, the CSC may consider changing CSP. The CSC may select another one from the CSPs ranked by security assessment. If the assessment validity o consecutively fails to meet the condition $o \geq \alpha$ for k times, the CSC may consider terminating the cloud service.

(2) Effectiveness. After determining that the validity meets the requirements, the CSC can set up an effectiveness indicator to determine whether the compliance level of cloud services meets its requirements. The effectiveness of compliance level is that the cloud services QoS can support critical business functions of CSC to an acceptable level within an evaluation period of time. Then, we define effectiveness as follows.

Input: set of evaluation period T, evaluation frequency t $(t \in T)$, monitoring frequency p, set of compliance metrics values C, set of QoS attributes A

1: **Data Collection and Preprocessing:** During the evaluation period T, monitor and record the actual data QoS attributes A in accordance with evaluation frequency of t and monitoring frequency p. Obtain the monitoring datasets D and categorize it into D_i $(D_i \in D)$ by each QoS attribute a_i $(a_i \in A)$. The dataset D_i can be further divided into D_i^j according to t_j.

2: **Compliance Interval Construction:** For the QoS attribute a_i, calculate the mean and variance of its monitoring dataset D_i^j. Then, construct the compliance interval according to the relevant features and approach of t-distribution.

3: **Single Conformance:** The single conformance v_{ij} of a_i can be calculated according to its compliance interval and compliance value c_i $(c_i \in C)$.

4: **Weight Assignment:** Applying entropy approach to determine the weight w_i^j for the single conformance v_{ij} of QoS attribute a_i. Calculate its weighted conformance by the obtained weight and single conformance.

5: **Compliance Level Evaluation:** Calculate the compliance level f_i of the QoS attribute a_i by aggregating its weighted conformance within evaluation period T. Repeat these steps above with each other attribute to obtain each compliance level of them.

Algorithm 3: Compliance Assessment.

Input: T, D_i, a_i, p, confidence level α, compliance metric value c_i

1: **procedure** Compliance Level Evaluation(D_i, T, p, α, C_i)
2: Create arrays $v^i_{1\times|T|}, m^i_{1\times|T|} \longleftarrow \emptyset$;
3: Create vector $\boldsymbol{w}^i_{1\times|T|}$;
4: $f_i \longleftarrow 0$;
5: **for** $j = 1$ to $|T|$ **do**
6: $v_{ij}, m_{ij} \longleftarrow$ SingleConformance (D_i, p, α, c_i);
7: **end for**
8: $\boldsymbol{w}_i \longleftarrow$ Compliance Weights Assignment (m_i);
9: **for** $j = 1$ to $|T|$ **do**
10: $f_i \longleftarrow f_i + v_{ij}\boldsymbol{w}_{ij}$;
11: **end for**
12: **return** f_i;
13: **end procedure**

Algorithm 4: Compliance Level Evaluation.

Definition 2. Let f denote the compliance level of a QoS attribute within an evaluation period T. Let n denote the number of QoS attributes. The effectiveness denoted as e can be calculated by

$$e = \frac{\sum_{i=1}^{n} f_i}{n} \tag{19}$$

The CSC can establish effectiveness threshold based on their actual business requirements. For instance, we assume that the acceptable effectiveness threshold of the CSC is β. Similarly, for a given evaluation period T (e.g., a year), the compliance assessment is performed in terms of t $(t \in T)$ (e.g., a day). If the effectiveness e is less than β, the CSC may consider seeking claims and remedies from the CSP. If the effectiveness e is greater than or equal to β, the CSC can use and evaluate the cloud service continuously.

In general, CSCs have to establish compliance tolerance rules based on their actual business requirements. In practice,

different CSCs may have different compliance tolerance rules. In this process, we provide a feasible and referential method for CSC to make decision according to the compliance level of cloud service.

5. Simulation Studies

This section presents the experiments to validate performance and availability of the proposed security and compliance assessment methods in the continuous assessment framework, respectively. The experiments are conducted by using MATLAB R2017b and performed on a DELL desktop computer with configuration as follows: Intel Core i5 2.7 GHz CPU,8 GB RAM and Windows 10 operating system.

5.1. Security Assessment Validation. First, we conduct the experiments to compare our security assessment method with the Quantitative Hierarchy Process (QHP) method proposed by [11] in terms of performance and accuracy. The QHP method is is an assessment technique that enables ranking of CSPs with respect to CSCs requirements. Due to the similar concepts and evaluation steps, we utilize the same security metrics as QHP, which are developed by Cloud Security Alliance [44]. For facilitating comparison, we employ the same quantification approach for security metrics as QHP. Additional, for convenience, we denote our security assessment method of SCCAF as SAM.

(1) Performance Analysis. To compare SAM with QHP method based on time complexity, we set the number of CSPs to 150 and the number of security metrics to 300. At the same time, we assume that each step in these comparative methods is an operation and the total number of operations represents the time complexity. We vary the number of CSPs from 1 to 150 with a step of 30 and the number of security metrics from 1 to 300 with a step of 60. We simulate that the time complexity of the two methods increases with the number of CSPs and the number of security metrics.

Figure 6 shows that the time complexity of the two methods increases with the number of CSPs in the case that the number of security metrics is constant. Figure 7 shows that the time complexity (operations) of the two methods increases with the number of security metrics in the case that the number of CSPs is constant. Figure 8 shows that the number of operations in both methods increases with the number of CSPs and security metrics. We can observe from these figures that our method outperforms QHP method in both above cases; that is, SAM has the minimum time complexity. With the increase of the number of CSPs or security metrics, the time complexity of QHP increases significantly. This is due to high complexity of algorithms for calculating the priority vector of comparison matrix constructed by all CSPs as per each security metric. In other words, QHP evaluates the security level of CSPs by comparing each security metric of all CSPs and aggregating the comparison results, while SAM is by taking all security indicators as a whole for comparison. It suggests that our method not only is effective but also outperforms QHP method.

(2) Accuracy of SAM. In order to validate accuracy of the SAM method, we compare evaluation results of SAM with evaluation results of QHP through empirical validation. Table 3 presents a sample dataset associated with security metrics used for this scenario. This dataset is excerpted by [11] from the information available in the CSA STAR repository [42], where the values associated to 16 security metrics for the three selected CSPs are presented. As aforementioned, for conveniently comparing the accuracy of both methods, we employ the same quantification approach for security metrics as QHP, which is described below. The selected security metrics comprised both qualitative (e.g., YES/NO) and quantitative (e.g., security levels from 1 to 4) metrics. The YES/NO metrics thresholds are modelled as Boolean 1/0, whereas metrics associated to security levels as $level_1$, $level_2$, $level_3$, and $level_4$ are modelled as 1, 2, 3, 4. For example, the CO3.3 is defined using qualitative thresholds (None, Annually, Quarterly, and Monthly) which are specified as $level_1$, $level_2$, $level_3$, and $level_4$. Similarly, the RI1.1 is defined using qualitative (Internal, External) values. To facilitate the comparison, we take the 16 security metrics in this table as the CSC's security requirements and consider them as the same relative importance ($weight = 0.5$) as described in *caseI* of [11].

In order to obtain the CSPs' security level, we apply the security assessment method presented in Section 5. Table 4 shows the parameters related to security level of CSPs, which are calculated by the algorithms elaborated in Section 5.1. As shown in Table 4, the shortest separation measure from alternative (CSP) to positive and negative ideal solution is CSP_3 and CSP_2, respectively. It means that for the given positive impact security metrics, CSP_3 is most consistent with them and CSP_2 is the most inconsistent with them. By taking the separation measures, we can obtain the relative closeness C of CSPs; the closer it is to 1, the higher the security level of the CSP is. As can been seen from this table, CSP_3 has the highest security level, followed by CSP_1, and CSP_2 is the lowest.

A side by side comparison is shown in Figure 9. As shown in Figure 9, the resulting ranking of CSPs is consistent for both SAM and QHP: CSP_3 is the provider that best satisfies the CSC's security requirements, followed by CSP_1 and CSP_2 respectively. For CSC specifying the security requirements, this means that both methods result in the same evaluation results. However, compared with the QHP method, the SAM method can better reflect the security level of CSPs. For example, in this scenario, since CSP_3 satisfies all the 16 security metrics, its security level should be the maximum, namely, 1, which is not shown in QHP.

5.2. Compliance Assessment Validation. In this section, we evaluate the availability and efficiency of the proposed compliance assessment method, which exploits a synthesized web service dataset from real world [53]. Additionally, we compare performance and certainty of our method with respect to the TRUSS proposed by [18]. For convenience, we denote our compliance assessment method of SCCAF as CAM.

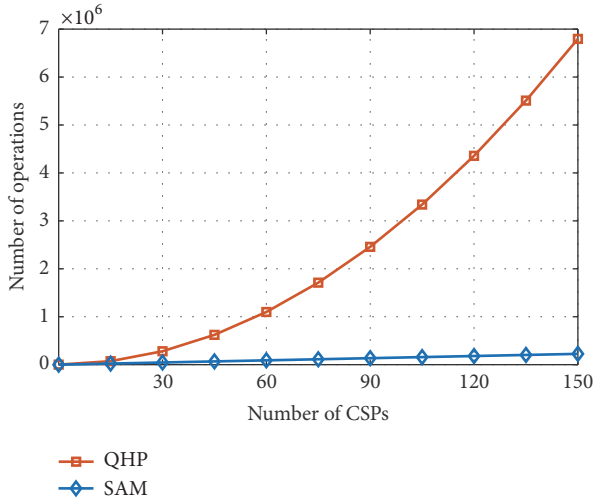


Figure 6: The operation comparison of SAM and QHP with respect to the number of CSPs.

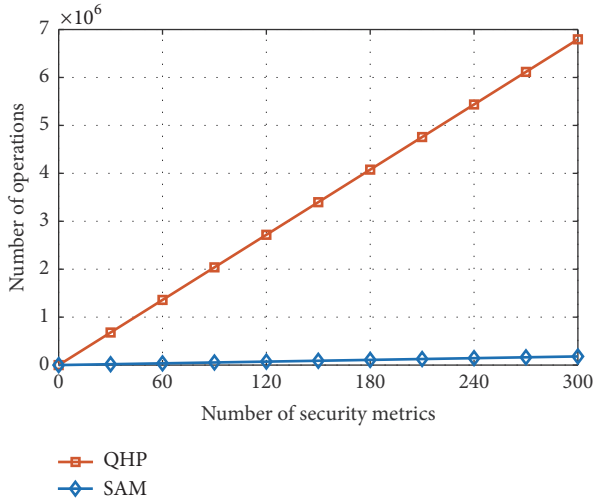
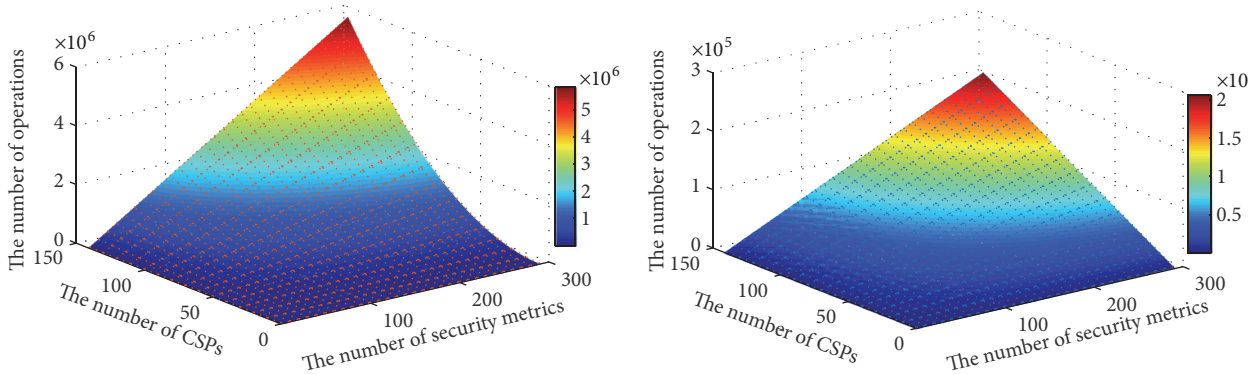


Figure 7: The operation comparison of SAM and QHP with respect to the number of security metrics.



(a) The number of operations of QHP

(b) The number of operations of SAM

Figure 8: The total number of operations comparison between SAM and QHP.

Table 3: Excerpt of CSPs security provisions based on CSCs security requirements [11].

Cloud security SLA element based on CSA STAR [42]			CSP_1	CSP_2	CSP_3
Control Category	Control Group	Security Metric		Value	
Compliance (CO)	Audit Planning (CO1)	CO1.1	*yes*	*yes*	*yes*
		CO1.2	$level_3$	$level_2$	$level_2$
	Independent Audits (CO2)	CO2.1	*no*	*yes*	*yes*
		CO2.2	*yes*	*yes*	*yes*
		CO2.3	*yes*	*yes*	*yes*
		CO2.4	*yes*	*yes*	*yes*
	Third Party Audits (CO3)	CO3.1	*yes*	*yes*	*yes*
		CO3.2	*yes*	*yes*	*yes*
		CO3.3	*Quarterly*	*Annual*	*Monthly*
Facility Security (FS)	Secure Area (FS1)	FS1.1	*no*	Monthly	*yes*
		FS1.2	*yes*	*no*	*yes*
	Asset Management (FS2)	FS2.1	*yes*	*yes*	*yes*
		FS2.2	$level_3$	$level_2$	$level_3$
		FS2.3	*yes*	*yes*	*yes*
Risk Management (RI)	Risk Assessments (RI1)	RI1.1	*Internal*	*Internal*	*External*
		RI1.2	*yes*	*yes*	*yes*

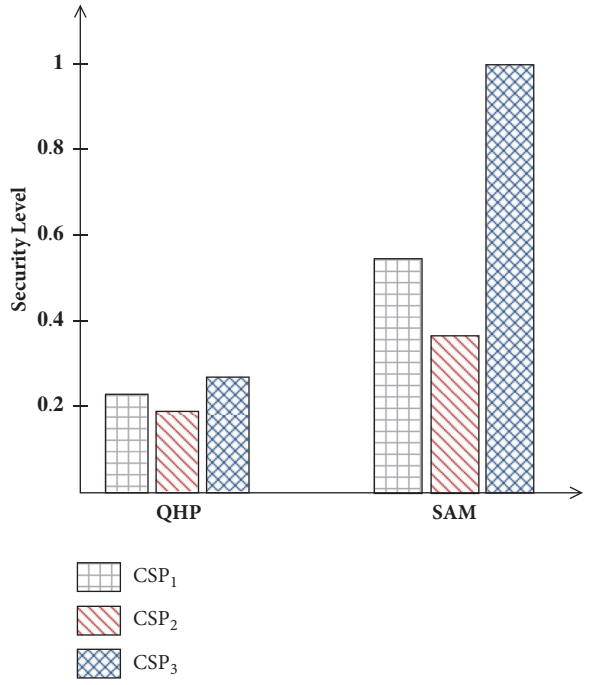


Figure 9: The security assessment results comparison of SAM and QHP.

Table 4: The separation measures and relative closeness of CSPs.

Alternatives		CSP_1	CSP_2	CSP_3
Separation Measures	D^+	0.3	0.43	0
	D^-	0.363	0.25	0.323
Relative Closeness	C	0.548	0.368	1

(1) Availability Validation. We utilize a real-world dataset to simulate the monitorable and measurable QoS attributes of cloud service and verify the availability and efficiency of CAM. This dataset, namely, WSDream dataset2, can be obtained from GitHub website [53]. It records a real-world QoS data from 142 users on 4,500 web services over 64 different time slices (at 15-minute interval). Each service has two QoS attributes in the original dataset, namely, response time (RT) and throughput (TP).

We denote the time slices and the number of users as the evaluation period (EP) and monitoring frequency, respectively. In addition, for facilitating the experiments, we

Table 5: Parameter settings.

QoS Attribute	Dataset	n	m	α	SLA
Response Time	RT_{mon}	64	118	0.05	2.219
Throughput	TP_{mon}	64	118	0.05	0.3901

identify 64 sets of QoS data in both RT and TP dataset, respectively, based on one single service from the original dataset (dataset2) via the keywords, namely, Time Slice ID. Each set contains 118 specific data values generated by users, which represents a set of monitored samples within an EP. As a result, we obtain two smaller QoS datasets, each containing 64×118 records and we denote them as RT_{mon} and TP_{mon}. We use these two datasets as the monitoring QoS value for compliance assessment in the experiments. The parameter settings are given in Table 5, where the number of items is denoted as m and the number of evaluation period is denoted as n. The *SLA* in this table denotes the compliance value with respect to the QoS attribute, which is described in Section 5.2. For convenience, we assumed that the SLA value of two QoS attributes are the mean of the RT_{mon} and the TP_{mon}, as shown in Table 5.

Let us now focus on the considered example. For the negative factor (RT), we first construct the compliance confidence interval according to a set of data in RT_{mon}, namely, the data in an EP. To facilitate the observation of the variation of the monitoring data in ideal case, we employ moving average method to process the monitoring data, which is denoted as smoothing data. Figure 10(a) illustrates the variation of the monitoring data of RT relative to its SLA and compliance confidence interval. As shown in Figure 10(a), the monitoring data vary around the SLA and its smoothing data basically vary within the compliance confidence interval. Because of the actual cloud environment, the QoS monitoring is a continuous process and its values are likely to vary due to the dynamics of the cloud resources (computing, network, and storage) and application workloads. Therefore, we denote the mean of monitoring data as the valid value to be evaluated in this EP. Similarly, Figure 10(b) shows the variation of the monitoring data of TP relative to its SLA and compliance confidence interval.

Then, we calculate the single conformance of RT in this EP according to the corresponding parameters, which includes SLA, compliance confidence interval, and the mean of monitoring data. The single conformance of RT in all EPs (64) can be obtained by the same way. Figure 11(a) shows that the single conformance of RT varies with the relationships across the confidence interval, SLA, and the mean intuitively. As shown in Figure 11(a), the confidence interval of RT does not fully cover the SLA; that is, there are some evaluation periods where RT is completely uncompliant. We can also conclude that the mean of RT varies around the SLA and always varies within the confidence interval. At the same time, it can be seen from this figure that the single conformance of RT is related to its confidence interval and the SLA, which varies between 0 and 1. In the case of a determined SLA, the single conformance of RT decreases with the increase of its confidence interval. When the upper limit of the confidence interval of RT is less than the SLA, the single conformance of RT is the maximum, namely 1. Conversely, the single conformance is the minimum value, namely 0, when the lower limit of the confidence interval of RT is less than the SLA. Similarly, Figure 11(b) shows the single conformance variation of TP.

Next, we determine the weights for the single conformance in each EP. The weight of single conformance of RT can be calculated according to (14), (15), and (16). Then we can use the obtained weights and the single conformance to calculate the weighted conformance of RT as well as TP in each evaluation period. Figure 12(a) shows the weighted single conformance of RT and TP. From this figure, we can observe that the single conformance of RT and TP in each EP is varying. Finally, we obtain the compliance level of RT and TP by aggregating their weighted single conformance in each EP, respectively. Figure 12(b) shows compliance level of RT and TP in form of the interval with every four EPs. From this figure, we can observe that the compliance level of RT and TP increases gradually over EP. This observation of results indicates that if the monitoring data of RT or TP is more stable and compliant over a period of time, its compliance level is closer to 1.

(2) Comparison with TRUSS. In this section, we compare our method of evaluating compliance with TRUSS [18]. The reason is obvious because of the similar direction of study on conformance evaluation of cloud service. Secondly, the sample dataset is derived from WSDream dataset2, so it becomes appropriate to compare both methods. Figure 13 illustrates the comparative computation function of QoS compliance evaluation between the two methods, which describes the effect of different weights and the single conformance on the compliance of an attribute in both TRUSS and CAM methods, respectively. As shown in Figure 13(a), the weighted conformance value varies with weight coefficient in TRUSS method, which means that the compliance computation function is excessively dependent on the weight. It is easy to cause the uncertainty of the conformance value. Figure 13(b) shows that the weighted conformance value has a certain relationship with the weight coefficient in CAM method, which means that the proposed method is more reasonable.

6. Conclusion

In this paper, we propose a new concept of cloud service life-cycle from the perspective of cloud-based IoT context, which enables CSCs to clearly understand the items that need to be considered at each phase of the adoption of cloud services. We have also presented a novel secure and compliant continuous assessment framework based on the cloud service life-cycle. This framework combines assessment methods of security and compliance as mutual complementation to facilitate CSCs to evaluate CSPs during the full cloud service life-cycle. Additionally, this assessment framework ensures the security of cloud-based IoT context by evaluating the security level and compliance level of cloud services. Simulation-based and case study experiments validated the performance and availability of our proposed method.

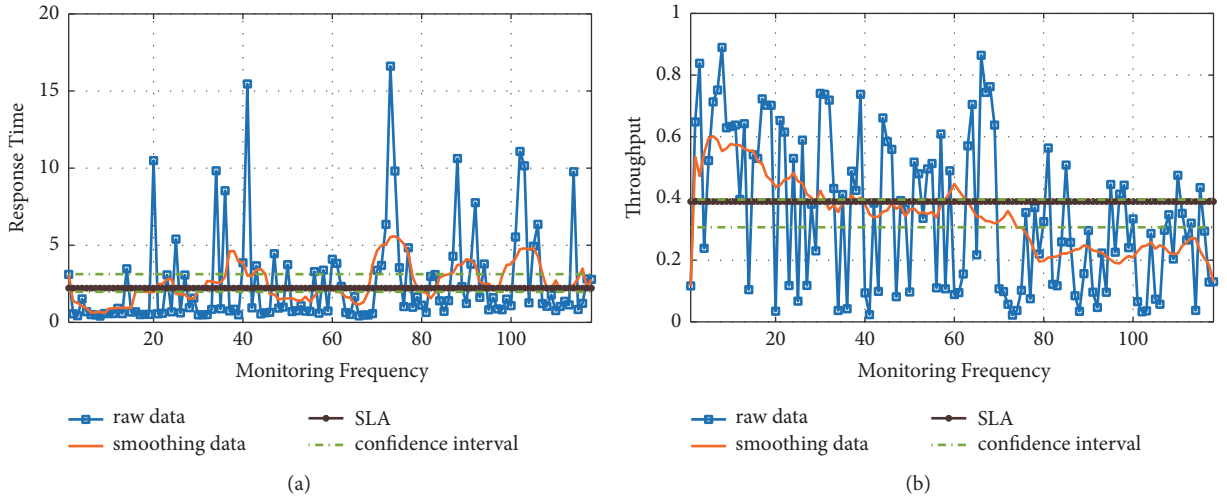


Figure 10: Monitoring data variation of RT and TP within t.

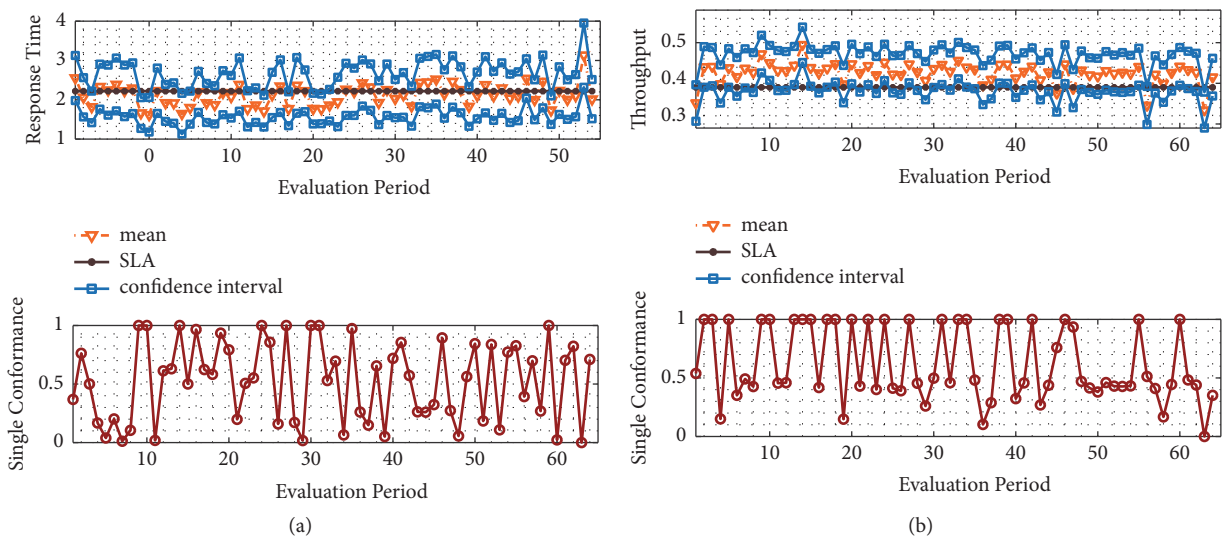


Figure 11: The single conformance o f RT and TP within T.

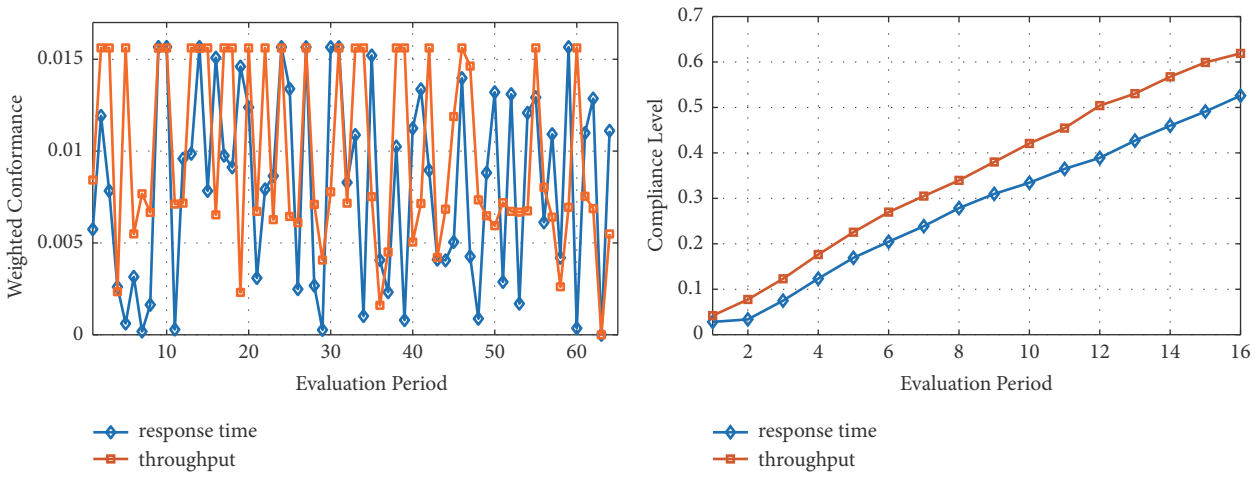


Figure 12: The compliance assessment results of RT and TP within T.

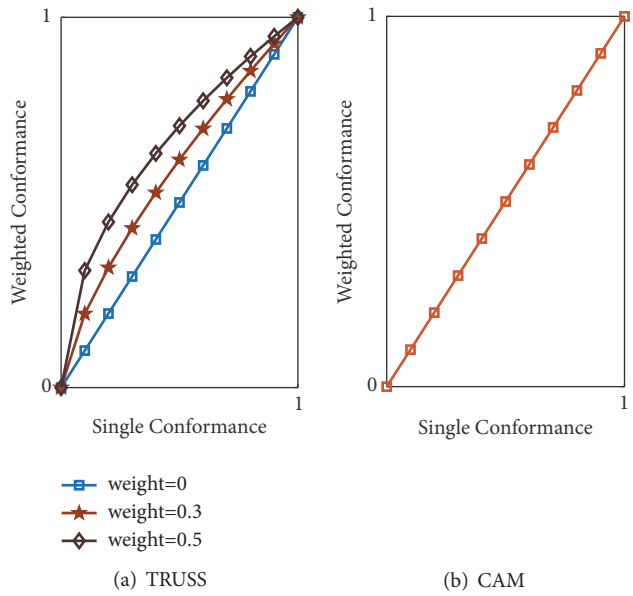


Figure 13: The compliance computation function comparison of CAM and TRUSS.

As future work, we plan extensions to the assessment framework in order to facilitate the evaluation of cloud service from the viewpoints of various stakeholders (e.g., cloud auditors, cloud brokers, or peers). We also plan to develop a prototype for our proposed assessment framework and further improve our evaluation algorithms.

Data Availability

The experimental data used to support the findings of this study are derived from the WSDream dataset2 repository (DOI:10.1109/TSC.2012.34.)

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grants 61802270 and 61802271 and in part by the Fundamental Research Funds for the Central Universities under Grants SCU2018D018 and SCU2018D022.

References

[1] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[2] D. Chen, N. Zhang, Z. Qin et al., "S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2017.

[3] N. Zhang, P. Yang, S. Zhang et al., "Software defined networking enabled wireless network virtualization: Challenges and solutions," *IEEE Network*, vol. 31, no. 5, pp. 42–49, 2017.

[4] D. Chen, N. Zhang, R. Lu, N. Cheng, K. Zhang, and Z. Qin, "Channel Precoding Based Message Authentication in Wireless Networks: Challenges and Solutions," *IEEE Network*, pp. 1–7.

[5] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4265–4276, 2015.

[6] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017.

[7] S. Singh, Y. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016.

[8] J. R. C. Nurse, S. Creese, and D. De Roure, "Security Risk Assessment in Internet of Things Systems," *IT Professional*, vol. 19, no. 5, pp. 20–26, 2017.

[9] Q. Wang, D. Chen, and N. Zhang, "LACS: A Lightweight Label-Based Access Control Scheme in IoT-Based 5G Caching Context," *IEEE Access*, vol. 5, pp. 4018–4027, 2017.

[10] Q. Wang, D. Chen, N. Zhang, Z. Ding, and Z. Qin, "PCP: A Privacy-Preserving Content-Based Publish-Subscribe Scheme with Differential Privacy in Fog Computing," *IEEE Access*, vol. 5, pp. 17962–17974, 2017.

[11] J. Luna, A. Taha, R. Trapero, and N. Suri, "Quantitative Reasoning about Cloud Security Using Service Level Agreements," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 457–471, 2017.

[12] J. Modic, R. Trapero, A. Taha, J. Luna, M. Stopar, and N. Suri, "Novel efficient techniques for real-time cloud security assessment," *Computers & Security*, vol. 62, pp. 1–18, 2016.

[13] T. Halabi and M. Bellaiche, "Evaluation and selection of Cloud security services based on Multi-Criteria Analysis MCA," in *Proceedings of the 2017 International Conference on Computing,*

Networking and Communications (ICNC), pp. 706–710, Silicon Valley, CA, USA, January 2017.

[14] S.-H. Na, K.-H. Kim, and E.-n. Huh, *A Methodology for Evaluating Cloud Computing Security Service-Level Agreements*, vol. 5, 2013.

[15] S. K. Garg, S. Versteeg, and R. Buyya, "SMICloud: a framework for comparing and ranking cloud services," in *Proceedings of the 4th IEEE/ACM international conference on utility and Cloud on utility and Cloud computing (UCC '11*, pp. 210–218, Melbourne, Australia, December 2011.

[16] Z. Ruo-xin, X.-j. Cui, S.-j. Gong, H.-k. Ren, and K. Chen, "Model for cloud computing security assessment based on ahp and fce," in *Proceedings of the in Computer Science Education (ICCSE, 2014 9th International Conference on. 1em plus 0.5em minus 0.4em IEEE*, pp. 197–204, 2014.

[17] S. Singh and J. Sidhu, "Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers," *Future Generation Computer Systems*, vol. 67, pp. 109–132, 2017.

[18] M. Tang, X. Dai, J. Liu, and J. Chen, "Towards a trust evaluation middleware for cloud service selection," *Future Generation Computer Systems*, vol. 74, pp. 302–312, 2017.

[19] S. Ding, S. Yang, Y. Zhang, C. Liang, and C. Xia, "Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems," *Knowledge-Based Systems*, vol. 56, pp. 216–225, 2014.

[20] J. Luna, H. Ghani, D. Germanus, and N. Suri, "A security metrics framework for the cloud," in *Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference*, pp. 245–250, 2011.

[21] J. Luna Garcia, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," in *Proceedings of the the 2012 ACM Workshop*, p. 103, Raleigh, North Carolina, USA, October 2012.

[22] V. Casola, R. Preziosi, M. Rak, and L. Troiano, "A reference model for security level evaluation: policy and fuzzy techniques," *Journal of Universal Computer Science*, vol. 11, no. 1, pp. 150–174, 2005.

[23] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-based quantitative approach for assessing and comparing cloud security," in *Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014*, pp. 284–291, China, September 2014.

[24] T. L. Saaty, "How to make a decision: the analytic hierarchy process," *European Journal of Operational Research*, vol. 48, no. 1, pp. 9–26, 1990.

[25] J. R. S. C. Mateo, "Multi-criteria analysis," in *Multi Criteria Analysis in the Renewable Energy Industry*, pp. 7–10, Springer, 2012.

[26] J. Abawajy, "Determining service trustworthiness in intercloud computing environments," in *Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks, I-SPAN 2009*, pp. 784–788, Taiwan, December 2009.

[27] M. Alhamad, T. Dillon, and E. Chang, "SLA-Based Trust Model for Cloud Computing," in *Proceedings of the 2010 13th International Conference on Network-Based Information Systems (NBiS)*, pp. 321–324, Takayama, Gifu, Japan, September 2010.

[28] Z. Xu, P. Martin, W. Powley, and F. Zulkernine, "Reputation-Enhanced QoS-based Web Services Discovery," in *Proceedings of the IEEE International Conference on Web Services (ICWS 2007)*, pp. 249–256, Salt Lake City, UT, USA, July 2007.

[29] Q. He, J. Yan, H. Jin, and Y. Yang, "ServiceTrust: Supporting Reputation-Oriented Service Selection," in *Service Oriented Computing and Applications*, vol. 5900 of *Lecture Notes in Computer Science*, pp. 269–284, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[30] S. S. Yau and Y. Yin, "QoS-Based Service Ranking and Selection for Service-Based Systems," in *Proceedings of the 2011 IEEE International Conference on Services Computing (SCC)*, pp. 56–63, Washington, DC, USA, July 2011.

[31] L. Zeng, B. Benatallah, A. H. H. Ngu, M. Dumas, J. Kalagnanam, and H. Chang, "QoS-aware middleware for Web services composition," *IEEE Transactions on Software Engineering*, vol. 30, no. 5, pp. 311–327, 2004.

[32] S. Kalepu, S. Krishnaswamy, and . Seng Wai Loke, "Reputation = f(user ranking, compliance, verity)," in *Proceedings of the Proceedings. IEEE International Conference on Web Services, 2004.*, pp. 200–207, San Diego, CA, USA, July 2004.

[33] L. Vu, M. Hauswirth, and K. Aberer, "QoS-Based Service Selection and Ranking with Trust and Reputation Management," in *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE*, vol. 3760 of *Lecture Notes in Computer Science*, pp. 466–483, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[34] S. S. Yau, J. Huang, and Y. Yin, "Improving the Trustworthiness of Service QoS Information in Service-Based Systems," in *Autonomic and Trusted Computing*, vol. 6407 of *Lecture Notes in Computer Science*, pp. 208–218, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[35] X. Liu, K. K. Fletcher, and Mingdong Tang, "Service Selection Based on Personalized Preference and Trade-Offs among QoS Factors and Price," in *Proceedings of the 2012 IEEE International Conference on Services Economics (SE 2012)*, pp. 32–39, Honolulu, HI, June 2012.

[36] Z. Zheng, H. Ma, M. R. Lyu, and I. King, "QoS-aware web service recommendation by collaborative filtering," *IEEE Transactions on Services Computing*, vol. 4, no. 2, pp. 140–152, 2011.

[37] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Future Generation Computer Systems*, vol. 29, no. 4, pp. 1012–1023, 2013.

[38] Z. Zheng, X. Wu, Y. Zhang, M. R. Lyu, and J. Wang, "QoS ranking prediction for cloud services," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1213–1222, 2013.

[39] M. Menzel and R. Ranjan, "CloudGenius," in *Proceedings of the the 21st international conference*, p. 979, Lyon, France, April 2012.

[40] A. Li, X. Yang, S. Kandula, and M. Zhang, "CloudCmp: comparing public cloud providers," in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement (IMC '10)*, pp. 1–14, ACM, Melbourne, Australia, November 2010.

[41] L. Huang, S. Deng, Y. Li, J. Wu, J. Yin, and G. Li, "A Trust Evaluation Mechanism for Collaboration of Data-Intensive Services in Cloud," *Applied Mathematics & Information Sciences*, vol. 7, no. 1L, pp. 121–129, 2013.

[42] *Consensus assessments initiative questionnaire, Cloud Security Alliance*, Standard, 2017.

[43] Information security technology-Security guide of cloud computing services, GB/T 31167-2014, National Information Security Standardization Technical Committee, 2014.

[44] Cloud Controls Matrix, *Cloud Security Alliance*, Standard, 2017.

[45] T. L. Saaty, "Decision making the analytic hierarchy and network processes (AHP/ANP)," *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83–98, 2008.

[46] M. Behzadian, S. K. Otaghsara, M. Yazdani, and J. Ignatius, "A state-of the-art survey of TOPSIS applications," *Expert Systems with Applications*, vol. 39, no. 17, pp. 13051–13069, 2012.

[47] ISO/IEC 19086-1, Information technology-Cloud computing-Service level agreement (SLA) framework-Part 1:Overview and concepts, International Organization for Standardization/International Electrotechnical Commission, 2016.

[48] ISO/IEC 19086-3, Information technology-Cloud computing-Service level agreement (SLA) framework-Part 3: Core conformance requirements, International Organization for Standardization/International Electrotechnical Commission, 2016.

[49] Cloud Computing Service Metrics Description, *National Institute of Standards and Technology, Standard*, 2018.

[50] ISO/IEC FDIS 19086-2, Information technology-Cloud computing-Service level agreement (SLA) framework-Part 2: Metric Model, International Organization for Standardization/International Electrotechnical Commission, 2017.

[51] B. V. Gnedenko, "Theory of probability. 1em plus 0.5em minus 0," *4em Routledge*, 2017.

[52] C. E. Shannon, "A mathematical theory of communication," *Bibliometrics*, vol. 5, no. 1, pp. 3–55, 2001.

[53] Z. Zheng, Y. Zhang, and M. R. Lyu, "Investigating QoS of real-world web services," *IEEE Transactions on Services Computing*, vol. 7, no. 1, pp. 32–39, 2014.

Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 5183451, 11 pages
https://doi.org/10.1155/2018/5183451

Research Article

The Improved Hill Encryption Algorithm towards the Unmanned Surface Vessel Video Monitoring System Based on Internet of Things Technology

Tingting Yang[1], **Yangyang Li**[1], **Chengzhe Lai**[2], **Jie Dong**[3], **and Minghua Xia**[4]

[1]*Navigation College, Dalian Maritime University, No. 1 Linghai Road, Dalian, Liaoning, China*
[2]*Telecommunication and Information Engineering College, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi, China*
[3]*Software College, Dalian University of Technology, China*
[4]*Electronics and Information Technology College, Sun Yat-Sen University, China*

Correspondence should be addressed to Tingting Yang; yangtingting820523@163.com

Received 19 June 2018; Accepted 10 September 2018; Published 3 October 2018

Guest Editor: Zhiqing Wei

Depending on the actual demand of maritime security, this paper analyzes the specific requirements of video encryption algorithm for maritime monitoring system. Based on the technology of Internet of things, the intelligent monitoring system of unmanned surface vessels (USV) is designed and realized, and the security technology and network technology of the Internet of things are adopted. The USV are utilized to monitor and collect information on the sea, which is critical to maritime security. Once the video data were captured by pirates and criminals during the transmission, the security of the sea will be affected awfully. The shortcomings of traditional algorithms are as follows: the encryption degree is not high, computing cost is expensive, and video data is intercepted and captured easily during the transmission process. In order to overcome the disadvantages, a novel encryption algorithm, i.e., the improved Hill encryption algorithm, is proposed to deal with the security problems of the unmanned video monitoring system in this paper. Specifically, the Hill algorithm of classical cryptography is transplanted into image encryption, using an invertible matrix as the key to realize the encryption of image matrix. The improved Hill encryption algorithm combines with the process of video compression and regulates the parameters of the encryption process according to the content of the video image and overcomes the disadvantages that exist in the traditional encryption algorithm and decreases the computation time of the inverse matrix so that the comprehensive performance of the algorithm is optimal with different image information. Experiments results validate the favorable performance of the proposed improved encryption algorithm.

1. Introduction

The Internet of things is widely used in intelligent transportation, environmental protection, government work, public safety, safe home, intelligent fire protection, industrial monitoring, environmental monitoring, street lighting control, landscape lighting control, building lighting control, square lighting control, square lighting control, elderly care, personal health, flower cultivation, water system monitoring, food traceability, enemy detection, and intelligence gathering. Based on the technology of Internet of things, the intelligent monitoring system of USV is designed and realized, and the security technology and network technology of the Internet of things are adopted. The intelligent perception of the self and environment information of the unmanned ship is realized by a variety of sensors. It is envisaged that developing an USV video monitoring system will greatly contribute to the maritime distress, urgency, safety, and general communications. The threat of maritime [1] piracy has mushroomed enormously in the past few years, especially in the detailed sea area below are piracy affected areas where the terror and threat of sea pirates have reached looming proportions: the strait of Malacca, the South China Sea, Gulf of Aden, and so on. The news channels on a daily basis have several incidents to report about pirates attacking crew and looting the vessel or hijacking a ship, and even causing

harm to the crew when their ransom demands are not met by the authorities. The maritime cloud server monitors the sea and collects a large amount of data [2–5] by USV video monitoring system; we will take timely and effective measures to deal with different situations by analyzing data. At the same time, it can collect information of a special area and obtain important information by this system, and experts can use these information to study whether the area can be expanded and whether there are available resources further. Video may be stolen and changed by pirates and other terrorists in the process of transmission that will pose a serious threat to information security of the sea; it is inconvenient to sea navigation, transportation, and any other activities of the sea. The encryption of video data has become priority, which is beneficial to the security of the sea and reducing losses and casualties.

With the development of information technology and the continuous progress of the society, there are more and more demands for information. Communication becomes convenient, quick and flexible by voice, data, image, and video in many ways at anytime and anywhere. In the past, the interaction of image and video information is a kind of extravagant demand for people, because of the limitation of network transmission technology and image compression ability. In recent years, with the increase of network bandwidth and the development of video image compression technology, people can carry out transmission of image and video through a variety of ways. In particular, with the progress of wireless transmission technology, the communication technology is affecting people's production and life in an unprecedented scale and degree [6]. The transmission of video and image information by wireless channels has become an urgent demand of application and the rapid improvement of network transmission technology; especially the wireless transmission technology could bring convenience to us, but it also brings hidden danger that sensitive image information may be stolen easily and spread illegally. Therefore, the security problem of image information has become a very important and crucial problem. Although the research of video encryption technology has been carried out for nearly 20 years, the existing secret strategy is not perfect and there is a large space for improvement, the encryption strategy of images transmitted under wireless conditions, whose degree of security is low. There are many different encryption methods and their respective systems have been formed but no performance of encryption strategy is satisfactory for all users. There are huge differences between various encryption strategies and the debates are hot. Video information security is an interdisciplinary subject spanning mathematics, cryptography, information theory, probability theory, computational complexity theory, and so on; it is related to video compression, network transmission, and application standards closely, which makes video encryption technology becomes a problem that has not been completely dealt with.

In this paper, a novel video encryption algorithm (i.e., Improved Hill encryption algorithm) is proposed, according to specific requirements of the wireless video monitoring system and combining with the research progress of video encryption technology. The algorithm combines with the process of video compression and regulates the parameters of the encryption process according to the content of the video image [4], so that the comprehensive performance of the algorithm is optimal for different image information. The results of the experiment are that the algorithm has good performance in the influence of adjacent pixels, and the information entropy of images is smaller than other algorithms. This work targets to investigate the security issues in maritime communication system, which is featured by protecting important data. Specifically, the contribution of this paper is threefold:

(1) We propose a novel video monitoring system of the USV to monitor the situation over sea, so that the authorities on the shore could obtain the video data in time and implement countermeasures for specific situations.

(2) A novel algorithm, namely, improved Hill encryption algorithm, is proposed, which has optimal comprehensive performance with respect to the security issue.

(3) It has been proved from the experimental results that the superior performance of the proposed improved Hill encryption algorithm.

The remainder of this paper is organized as follows. In Section 2, we discuss some related works. System model is presented in Section 3. The improved encryption algorithm is proposed, and the performance analysis is corroborated in Sections 4 and 5, respectively. In Section 6, we summarize the flow and indicate how the performance of the algorithm is improved.

2. Related Work

In recent years, driverless cars and UAV are becoming ever more popular among the public. Google Corporation is a pioneer in the field of research and development of driverless vehicles; the company announced that its unmanned vehicle project was developing to automated direction that is exclusion of human intervention at the end of May 2015 year. The prototype test of the automatic driverless vehicle will be carried out; it is expected that test of driving on the road can be carried out in a few years. At present, Google is making about 100 automatic vehicle models; UAV are striving to enter into people's lives, too. According to foreign media reports, online shopping giant Amazon is seeking permission from the US government to launch UAV flight test in the US. In fact, the research and exploration of USV are in progress in the field of unmanned technology, and ships floating on the sea will probably enter the unmanned era in the future. British Rolls Royce company (Luo Luo) is optimistic to this, as one of the [7] world's largest engine makers and shipbuilders who are determined to develop unmanned vehicles and offshore USV. There are slender difficulties in improving the unmanned craft at the technical level, and now there are many ships equipped with automatic equipment. The era of USV is seen in the future. Oscar Levand think that "In the near future, the USV will keep pace with the unmanned drones, the submarines and the unmanned vehicles that are being tested by Google". As far as water is concerned, the demand

of USV is strong. For example, while working on cruise and search, driverless technology can increase the number of ships that because it does not have to be manned and the size is small, its reaction is more responsive. To monitor the condition of the sea and collect important information by USV, once ships were attacked by pirate or the terrorist during the voyage, using video to capture the locations, numbers, features of the pirates, use of weapons equipment, and other important information, the information is transmitted to shore with unmanned vessel monitoring system. It should set a fixed time to transfer the collected information to the shore, it is convenience for shore personnel access to valid information in good time. Video should be sent to shore forcibly and take action in time in an emergency. The video data must be secure enough, once the data were intercepted and tampered that not only miss the best time to rescue and lose strong evidence.

In the multimedia computer technology application system, there are two research directions of video image processing. One is the compression encoding of the video image; the other is real-time processing of video image and protection of video information. In the video image compression algorithm, H.264 compression [8] algorithm as an international standard, because it has higher compression and it is able to provide a high quality image and supported by most of the operating platform, it also has good compatibility. H.264 has the following advantages: (1) coding efficiency: H.264 saves nearly 0.5 of its bandwidth compared with its predecessor H.263 and MPEG-4. (2) Superior quality images: H.264 can provide video images of high quality in low bit rate and image transmission of high quality on lower bandwidth is the highlight of H.264 application. (3) Improving network adaptability: H.264 can work in low delay mode under the real-time communication applications (such as video conferencing) and can also work in video storage or video streaming server that without delay. (4) Using hybrid coding structure: H.264 like previous H.261, H.263 use the hybrid coding structure, which is DCT transform coding and DPCM differential coding. At the same time, in order to improve the efficiency of compression coding, H.264 introduces a new coding methods under the structure of mixed coding, which adds new encoding methods, such as multimode motion estimation, intraprediction, and multiframe prediction, its content is based on variable length coding and 4x4 two-dimensional integer transform and improves the efficiency of coding. (5) H.264 has less coding options: a considerable number of options are often required to encode in H.263 that adds difficulty of coding, while H.264 achieves a concise "regression base" that reduces the complexity of the coding. (6) H.264 can be applied in different situations: H.264 can use different transmission and playback rates according to different environments and provide a rich tool of error handling that can control or eliminate the packet loss and bit error. (7) Error recovery function: H.264 provides a tool to solve the problem of network transmission packet loss, which is adapted for transmitting video data in a wireless network with transmission of high bit error rate. (8) Higher complexity: performance boost of H.264 is achieved at the expense of increasing complexity; it is estimated that the computational complexity of H.264 encoding is three times more than H.263 and the decoding complexity is twice as much as H.263.

The protection of video image information is to prevent sensitive information from being stolen and altered easily, copied, and disseminated illegally, including information encryption technology and information hiding. The encryption algorithm is built on the design of text data, the implementation of encryption that converts meaningful cleartext into meaningless ciphertext that is to prevent the information obtained during the process of data transmission by illegal interceptors. Video file has the characteristics of large data volume and require extraordinary real-time requirements, so it is difficult to gratify the requirements of video information on encryption efficiency that use traditional encryption algorithms sometimes. Spatial image encryption is encrypting the gray [9] scale of the image, because the gray scale (pixel value) of the image is the byte data that can be encrypted by means of data encryption. Therefore, the data encryption algorithm can be transplanted into gray scale encryption algorithm, which includes data encryption standard, simple Hill matrix encryption, and sequence encryption algorithm. In this paper a new image encryption algorithm is proposed that is based on the traditional Hill algorithm; we use an invertible matrix as a key to encrypt the image matrix and then transpose the encrypted image. Besides, the final step is double-layer encryption of matrix.

3. System Model

In this paper, we propose to use the LAN technology of Internet of things to construct the unmanned video monitoring system, the video node is connected with the different monitors of the USV through the local area network, and the control center can communicate with the maritime cloud service center that achieve the effect of information sharing. Compared with other methods, it has an advantage that it can be applied to USV of different sizes, so that we can design the USV video monitoring system according to the USVs size and structure, it just only to change the number of video monitoring nodes and location on the base of different requirements. The unmanned video monitoring system focuses on the security of ship navigation and cargo transportation. Monitoring the different locations over surface by configuring a certain number of cameras and other technological means, the information will be compressed and encrypted by SecurCore processor of DSP core and transmitted with three ways Figure 1. When the distance is far, the communication will be achieved by satellite and cloud platform and other shore-based or air-based facilities. We can select the corresponding schemes according to the distance, which saves the cost, decreases the time of communication, and avoids the waste of resources. The specific information transmission paradigms are shown in Figure 2.

3.1. Video Acquisition Module. The acquisition module of the video data is the input stage of information and its performance is very important to the whole system; the

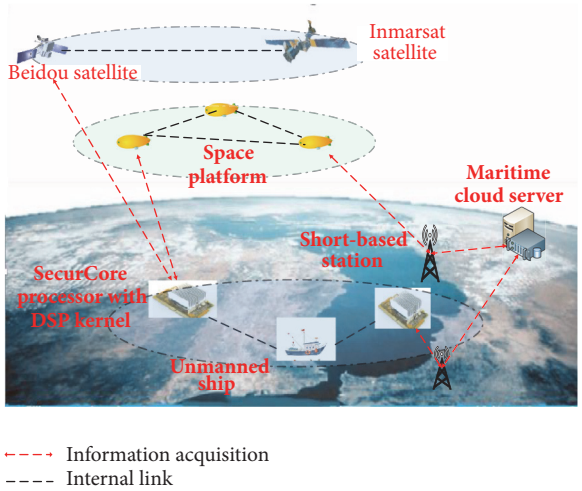


Figure 1: Information transmission diagram.

quality of the original video and image will determine the final image clarity of the maritime cloud server; the marine environment can be detected by sensors at sea, such as temperature sensors and thermosensitive components, light sensors and photosensitive elements, gas sensors and gas sensors, magnetic sensor, and subsensitive element. In this paper the module includes camera and corresponding control parts. The monitoring contents include the travel records of the ships and the meteorology of the sea as well as the transportation security of the goods and so on, it can also store and print pictures as the important evidence.

3.2. Video Compression and Encryption Module. The compression and encryption module of the video are the core of the unmanned video monitor system and its performance affects the overall performance of the system directly. The compression of video data is limited by various conditions, such as the transmission bandwidth, image resolution, frame rate, maximum delay of coding, and performance of processor. Therefore, the video compression module has to be coordinated with the transmission module, the encryption is integrated into the compression, and their relationship is very close. The module of compression and encryption can be implemented by SecurCore processor of DSP core.

3.3. Video Transmission Module. While the video data is completed by the hardware compression and it needs to be sent to the service platform through the network. However, there will be a few problems in the processing of sending, such as the simultaneous transmission of multiple monitoring nodes or the blockage of the network; it may occur that data is lose. In the process [10] of data transmission the network will judge the size of the packet, when the size is more than or less than the certain limit the packet will be discarded, the exact scope is (64-1500) bytes. RTP protocol is used to transmit video files because it is a real-time network transmission protocol that is often used for single point data transmission and it is very suitable for the transmission of audio and video data.

3.4. Video Playback Module. In the system, the shipboard service center needs to play video and image; according to their different purposes, the implementation is adopted by different ways. The purpose of the video broadcast of the VSV adjusts the camera easily, so that it can make tracking the target better. On the maritime cloud server, the purpose of the playing video is to have a clear understanding of the experiment site and analysis things what happened after that. Therefore, the image definition must be distinguished and should be enhanced before playing.

3.5. Video Storage Module. It is a part of the important functions of the system that the storage of video data during the experiment process, to analyze the situation of the experimental field after the experiment is possible. The maritime cloud server center is analysis and disposing center of the experimental data that has intense computing power and large storage space; it is appropriate to backup and long-term archival of experimental data. The transmission of data can be reduced by using the mode of maritime cloud server center storage. However, the data obtained by USV are transmitted by the wireless channel, and the noise and interference are unavoidable. After being processed a few steps, the data will increase the corresponding noise of process. The definition of video image is the most important index of the system, in order to archive the data of high quality and remove unnecessary noise and interference, the video data will be stored in the USV board monitoring platform.

4. Improved Hill Encryption Algorithm

The idea of Hill algorithm is to convert l cleartext letters into l ciphertext letters by a series of linear transformations, the decryption only requires one inverse transformation [11], and the key is the transformation matrix itself. Hill password is a part of the multiple-letter substitution codes and it is also called the matrix transformation password. The vector of cryptograph is $C = KM(\mathrm{mod}N)$

$$C = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_l \end{bmatrix} \tag{1}$$

$$M = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_l \end{bmatrix} \tag{2}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{3}$$

$$K = \left(k_{ij}\right)_{l\times l} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1l} \\ k_{21} & k_{21} & \dots & k_{2l} \\ \vdots & \vdots & & \vdots \\ k_{l1} & k_{l2} & \dots & k_{ll} \end{bmatrix} \tag{4}$$

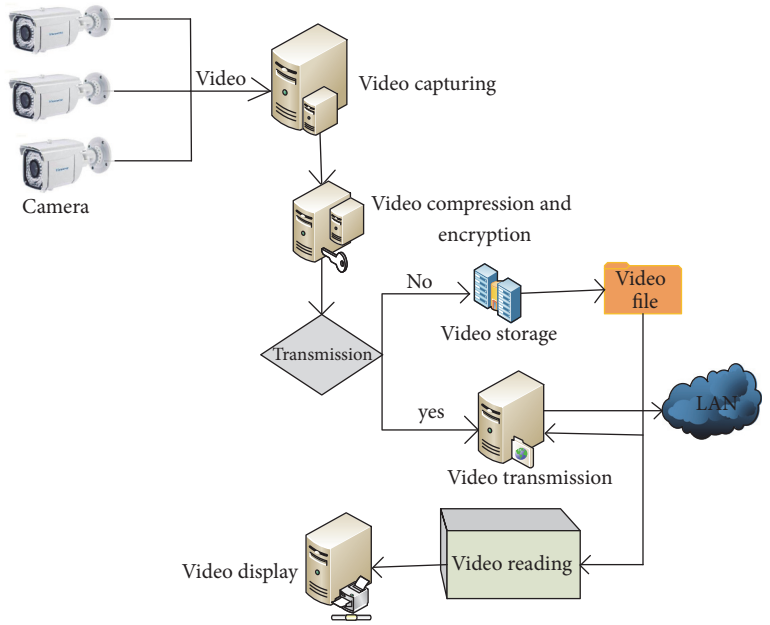


Figure 2: Flowchart of information processes.

In the formula, C is ciphertext and M is cleartext and the key K is an invertible matrix. The decryption formula is $M = K^{-1}C(\text{mod}N)$. All the arithmetic operators are performed under the mode of $N = 26$.

Example 1. Suppose the key $K = \left[\begin{smallmatrix} 6 & 7 \\ 3 & 8 \end{smallmatrix}\right]$; while the encryption comes true by using the Hill password, according to the above calculation we can get a result that $K^{-1} = \left[\begin{smallmatrix} 8 & 19 \\ 23 & 6 \end{smallmatrix}\right]$. Suppose that the "good" is cleartext to be encrypted, then the cleartext is divided into two groups that (6,14) is "go" and (14,3) is "od". The process of encryption is

$$\begin{aligned} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} &= K \begin{bmatrix} m_1 \\ m_2 \end{bmatrix} = \begin{bmatrix} 6 & 7 \\ 3 & 8 \end{bmatrix} \bullet \begin{bmatrix} 6 \\ 14 \end{bmatrix} (\text{mod}26) \\ &= \begin{bmatrix} 134 \\ 130 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 4 \\ 0 \end{bmatrix} \\ \begin{bmatrix} c_3 \\ c_4 \end{bmatrix} &= K \begin{bmatrix} m_3 \\ m_4 \end{bmatrix} = \begin{bmatrix} 6 & 7 \\ 3 & 8 \end{bmatrix} \bullet \begin{bmatrix} 14 \\ 3 \end{bmatrix} (\text{mod}26) \\ &= \begin{bmatrix} 105 \\ 66 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 1 \\ 14 \end{bmatrix} \end{aligned} \tag{5}$$

The result of encryption is "EABO". The process of decryption is

$$\begin{aligned} \begin{bmatrix} m_1 \\ m_2 \end{bmatrix} &= K^{-1} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 8 & 19 \\ 23 & 6 \end{bmatrix} \bullet \begin{bmatrix} 4 \\ 0 \end{bmatrix} (\text{mod}26) \\ &= \begin{bmatrix} 32 \\ 92 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 6 \\ 14 \end{bmatrix} \\ \begin{bmatrix} m_3 \\ m_4 \end{bmatrix} &= K^{-1} \begin{bmatrix} c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 8 & 19 \\ 23 & 6 \end{bmatrix} \bullet \begin{bmatrix} 1 \\ 14 \end{bmatrix} (\text{mod}26) \\ &= \begin{bmatrix} 274 \\ 107 \end{bmatrix} (\text{mod}26) = \begin{bmatrix} 14 \\ 3 \end{bmatrix} \end{aligned} \tag{6}$$

Get the correct cleartext in the last.

4.1. Self-Invertible Matrix. In the encryption formula, K has inverse matrix K^{-1} and $(K^{-1}K)M = M = K^{-1}C(\text{mod}26)$, which is possible to realize the decryption. Essentially, using the invertible matrix K is important when you encrypt/decrypt. How do you see a matrix can be invertible? It depends on the determinant that is [12] nonzero (all of the above operations are performed under mode $N = 26$). So we know that the invertible matrix K has the inverse of the mode of $N = 26$, only if $GCD(\det K, 26) = 1$. Here, we use the $GCD(x, y)$ to denote the largest common divisor of the integer x and the integer y, using $\det K$ or $|K|$ to represent the determinant of the matrix K. The Hill encryption algorithm is applied to the image matrix P to get the corresponding Hill image encryption algorithm; the encryption process is $C = E_k(P) = K \bullet P$, and decryption process is $P = D_k(C) = K^{-1} \bullet C = K^{-1} \bullet K \bullet P = P$.

The basis of the algorithm is as follows.

If matrix A satisfies $A = A^{-1}$, then A is called a self-invertible matrix. Assumptions

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \vdots & a_{nn} \end{bmatrix} \tag{7}$$

It is $n \times n$ self-invertible matrix, n is even, and suppose $n = 2$, then it is written as

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \tag{8}$$

In the formula, $A_{11}, A_{12}, A_{21}, A_{22}$ are $(n/2) \times (n/2)$ matrices. Result from the self-reversibility of A are

$$A \bullet A = A \bullet A^{-1} = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} = I \tag{9}$$

Result from formula (8) is

$$A_{12}A_{21} = I - {A_{11}}^2 = (I - A_{11})(I + A_{11}) \tag{10}$$

According to formula (9), $|A_{12}|$ is a factor of $|I - {A_{11}}^2|$ and $|A_{21}|$ is another factor. Suppose there is a constant k

$$A_{12} = k(I - A_{11}) \tag{11}$$

Then

$$A_{21} = \frac{(I + A_{11})}{k} \tag{12}$$

From formula (11) we can get second matrix equations

$$A_{11}A_{12} + A_{12}A_{22} = 0 \tag{13}$$

When formula (10) is established, $|A_{11}|$ and $|A_{12}|$ will be exchanged

$$\begin{aligned} A_{11}A_{12} &= A_{11} \bullet k(I - A_{11}) = k(I - A_{11}) \bullet A_{11} \\ &= A_{12}A_{11} \end{aligned} \tag{14}$$

Formulae (13) to (12) obtain

$$A_{12}A_{11} + A_{12}A_{22} = A_{12} \bullet (A_{11} + A_{22}) = 0 \tag{15}$$

while $A_{12} \neq 0$ get the result

$$A_{11} + A_{22} = 0 \tag{16}$$

The self-reversible matrix algorithm is obtained.

The algorithm steps are as follows:

(1) Choose $(n/2) \times (n/2)$ matrix A_{22} arbitrarily.

(2) Get the result by a series of calculations that $A_{11} = -A_{22}$.

(3) Take $A_{12} = k(I - A_{11})$ or $k(I + A_{11})$ and k is a prime number.

(4) Count $A_{21} = (I - A_{11})/k$ or $A_{21} = (I + A_{11})/k$.

(5) Merge into a complete matrix.

4.2. Improved Hill Encryption Scheme. The steps of improved Hill encryption algorithm are as follows.

Step 1. $m \times m$ self-reversible matrix is generated as the key matrix of this algorithm.

Step 2. Divide the original image into $m \times m$ block image.

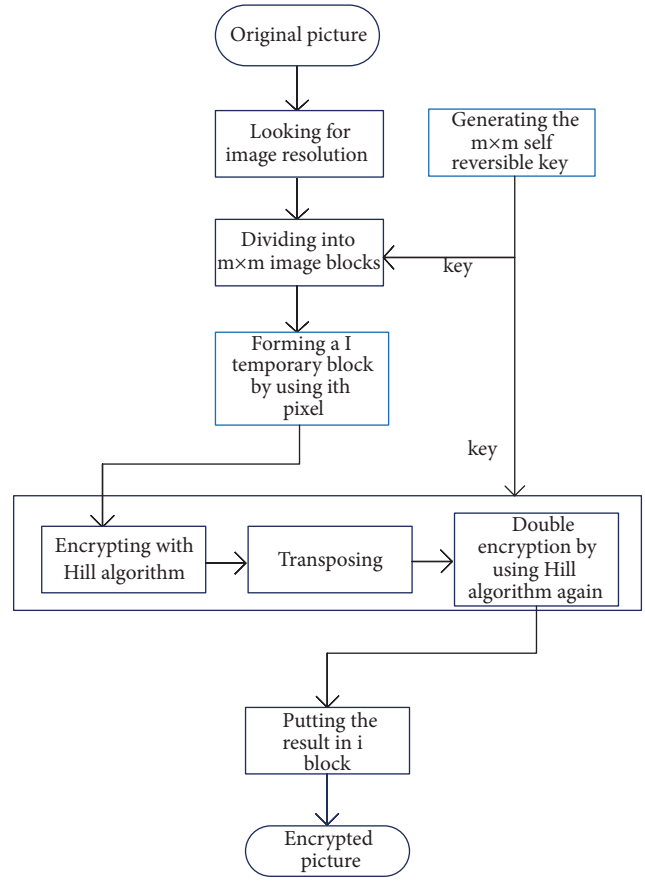


Figure 3: Flowchart of encryption.

Step 3. The i pixels of each image block will be grouped together and made up $m \times m$ temporary image block, it is convenient for future encryption operation.

(1) The temporary image matrix is encrypted with the key matrix A.

(2)Transpose the encrypted image matrix and double-layer encrypting the matrix.

Step 4. Putting the obtained matrix into the ith position of the final encryption matrix.

The process of decryption is the reverse process of encryption; the block diagram of the specific encryption algorithm is shown in Figure 3.

4.3. Security Analysis of Hill Algorithm. The key conditions of Hill encryption algorithm are character information and digital correspondence table and encryption matrix. Character information and number correspondence table representation: the larger the order of the encryption matrix is, the more difficult it is to decipher and the amount of calculation. The definition of the encryption matrix and the solution of the matrix are also very important to [13] encryption and decoding of the algorithm. From the point of cryptanalysis code, using traditional passwords to encrypt video has a lot of drawbacks; the broken translator can sum up the analogous

Table 1: Adjacent pixel.

direction	Artwork	Hill encryption	Article encryption
level	0.902985	0.329121	-0.005825
vertical	0.874309	0.227804	0.008831
diagonal	0.856915	0.173428	-0.030353

rules from the statistical string frequency and find out the exit of cryptanalysis. With the rapid development of science and technology, the deciphering time is less than before. But Hill encryption algorithm [14] uses matrix multiplication and inversion in linear algebra, it is better to resist frequency analysis, and it is difficult realizing the decoding. Hill encryption algorithm has set up three handicaps for the translator, which is incomprehensible to decipher. Because you do not know anything about that dimension variables of the text conversion, order of the corresponding letters, access method of the encryption matrix, if you want to decipher the code you should guess the three things correctly at least. But it is difficult to guess correctly at the same time. There is no password that can not be broken completely, and the Hill algorithm is no exception. Generally speaking, it is difficult decoding that only knows the attack of ciphertext, but it is easy to be broken by using attack of cleartext. Assume that the opponent already knows the value L and it also mastered l different tuples L at least. $M_i = \begin{bmatrix} m_{1i} \\ m_{2i} \\ \vdots \\ m_{li} \end{bmatrix}$, $C_i = \begin{bmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{li} \end{bmatrix}$, $1 \le i \le l$ The conditions were fulfilled that $C_i = E(M_i, K) = e_K(M_i)(1 \le i \le l)$. Defining two matrices that are $M = (m_{ij})_{l\times l}$ and $C = (c_{ij})_{l\times l}$, then has a matrix equation $C = K \bullet M(\text{mod}26)$. In the formula, $l \times l$ matrix K is an unknown key. If the M is reversible that can be calculated, $K = C \bullet M^{-1}(\text{mod}26)$. Thus the encryption algorithm is broken (if M is not reversible, we must try another cleartext-ciphertext pair). From the overall result Hill algorithm is still a simple and efficient algorithm.

5. Experimental Results and Analysis

In order to test the correlation between the two pixels adjacent to the vertical, adjacent, horizontal, the following tests are performed. Firstly, 1000-3000 pairs of pixels adjacent to the horizontal, vertical, and diagonal direction are randomly selected from the graph, and the correlation formula is used to calculate the correlation [15].

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(y)}\sqrt{D(x)}} \tag{17}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{18}$$

$$\text{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))((y_i - E(x)) \tag{19}$$

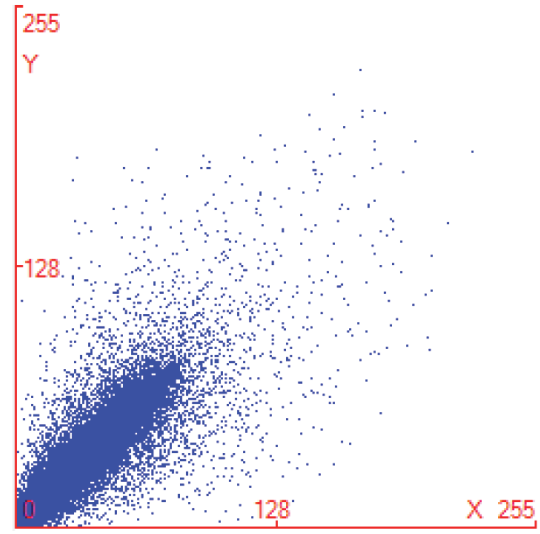


Figure 4: Correlation distribution diagram of original image.

In the formula, x and y are the gray values of two adjacent pixels in the image. $E(.)$, $D(.)$, and cov(.)are the expectation, variance, and covariance, respectively, and r is the correlation [14] coefficient of adjacent two pixels. The higher the value of its value is close to 1, the higher the correlation of adjacent pixels is. If images were encrypted by Hill self-invertible matrix encryption algorithm and improved algorithm, respectively, then compare the correlation between adjacent pixels in 3 directions.

$$UACI = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|C_1(i, j) - C_1(i, j)|}{255 \times M \times N} \times 100\% \tag{20}$$

The related data of Table 1 show that the adjacent pixels of the original image are large data, the correlation coefficient is close to 1 that can be seen, the adjacent pixels are highly correlated, the pixels correlation of traditional Hill encryption algorithm is around 0.2, but improved algorithm is more precise in reducing the correlation of adjacent pixels, making the size of data close to 0. From the correlation of adjacent pixels that improved encryption algorithm is much better than traditional Hill encryption algorithm.

Figures 4 and 5 represent the correlation distribution diagrams of two horizontal adjacent pixels in the original and traditional Hill encryption images, and the correlation distribution of Figure 5 is more diffuse than Figure 4, but the correlation distribution between the original image and the traditional Hill encryption image is not obvious enough. Figure 6 shows the improved algorithm encryption image, the

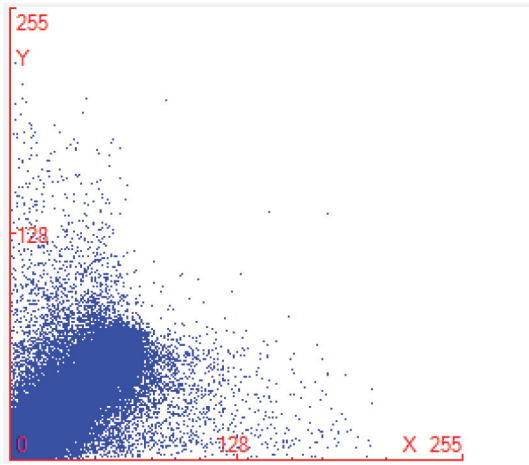


Figure 5: Correlation distribution of Hill encryption algorithm.

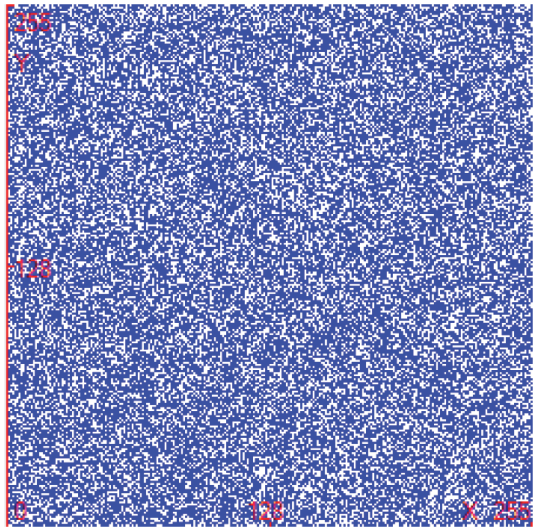


Figure 6: Correlation distribution of improved encryption algorithm.

comparison [16] between Figure 6 and Figure 5 shows that the correlation distribution is separate completely. From the analysis of the distribution degree of correlation graph, it is shown that the improved encryption algorithm is better than traditional Hill encryption algorithm.

5.1. Histogram Analysis of Encrypted Image. The variance is used to evaluate the consistency of histogram distribution and indicate the degree of dispersion between the histogram and its average value; the consistency of the distribution is expressed by the size of variance value. The smaller the variance the more uniform the distribution. The histogram of image is represented by $hist_i$, and the formula of variance is

$$S = \frac{1}{256}\sum_{i=0}^{255}\left(hist_i - aver\right)^2 \tag{21}$$

Figure 7: Original image.

and the *aver* is

$$aver = \frac{1}{256}\sum_{i=0}^{255} hist_i \tag{22}$$

The pixel value can be distributed evenly that, in the range of (0-255) after encryption, the uniform distribution of gray histogram will be regarded as the ideal state. From the above three images, it is found that the histogram (Figure 8) of the original image (Figure 7) is uneven, the uniformity of distribution is not ideal, the distribution effect (Figure 10) of the traditional Hill encryption image (Figure 9) has not been improved obviously, which has poor performance, and the pixels correlation of the image is not weakened. Compared with the traditional Hill encryption histogram, the histogram (Figure 12) of the improved algorithm encryption image (Figure 11) is more concentrated and more gentle. The value of the variance is obviously smaller than variance of the traditional Hill encryption algorithm, which weakens the correlation greatly and its result is ideal.

5.2. Information Entropy and Diffusivity Test. **Information entropy** is a concept used to measure the amount of information in information theory, which contains information content of an image, the system is more orderly that information entropy is more low. The information entropy of the image is

$$H\left(m\right) = -\sum_{i=0}^{L-1} p\left(m_i\right)\log_2 p\left(m_i\right), \qquad \sum_{i=0}^{L-1} p\left(m_i\right) = 0 \tag{23}$$

L and mi in the formula indicate that gray value is mi and description is L; P_{mi} indicates the probability of the appearance of gray value. When the probability that gray value appears in the image is equal, information entropy of

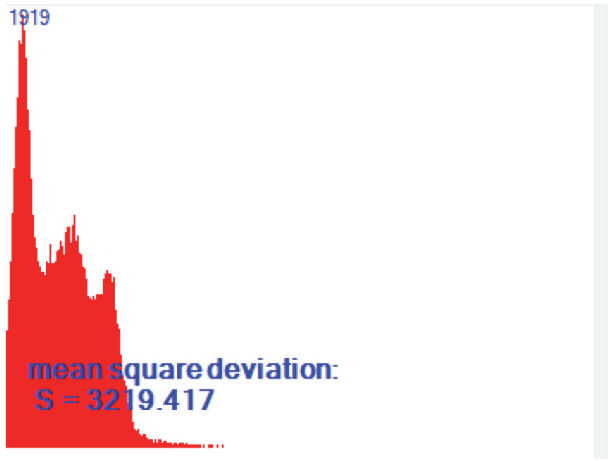


Figure 8: Histogram of original image.

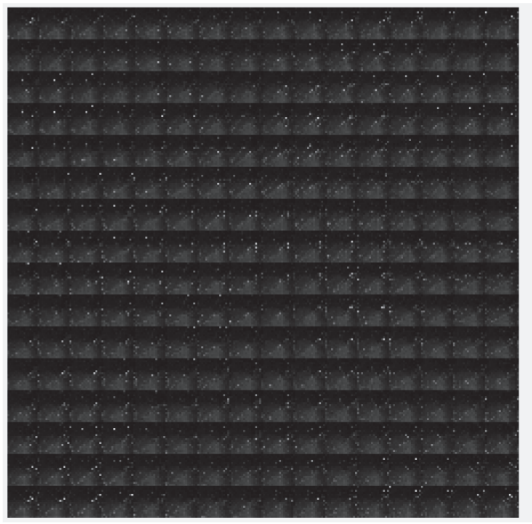


Figure 9: Hill encryption image.

the image is the largest, and its gray distribution is identical. When information entropy is equal to 8, that proved the fact that the random distribution of images is more ideal.

Diffusion is an important nature in the encryption algorithm that is proposed by Shannon in a document; an excellent encryption system must have good diffusivity. The meaning is that when a bit is changed in the original image, the encryption image will be changed in an unpredictable way. The diffusivity of the image encryption algorithm indicates that the output pixels of the encrypted image [17] should be dependent on the input pixels of the original image in a very complicated way, which can resist the attacker's analysis of the algorithm. Attackers usually make small changes to the original image and then use the algorithms used as attackers to encrypt the original and modified images and compare the relationship between the original and the encrypted images by comparing two images. This kind of attack becomes a difference attack [18]. One pixel of the original image is modified by the attacker; looking at the changes in the result,

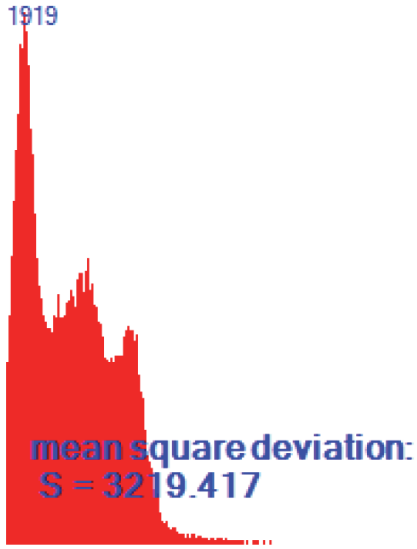


Figure 10: Histogram of Hill encryption image.

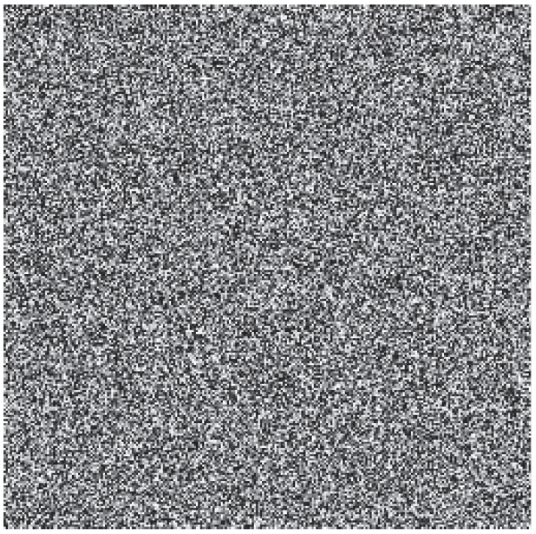


Figure 11: Improved Hill encryption image.

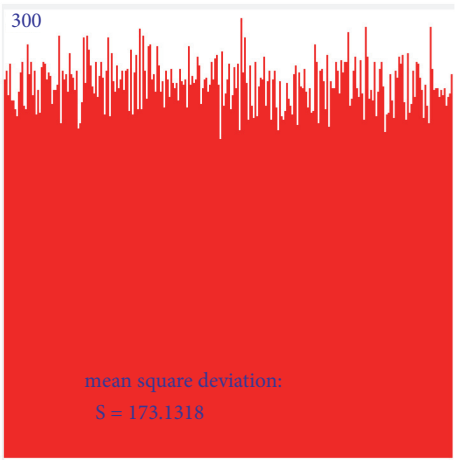


Figure 12: Histogram of improved Hill encryption image.

Table 2: Analysis of test results.

information	Artwork	Hill encryption	Article encryption
entropy	6.234655	6.234655	7.997266
NPCR	0.00	0.00001526	0.00024424
UACI	0.00	0.000015019	0.001794146

it is possible for attacker to find a relationship between the original image and the encrypted image. If a small change in the original image can cause significant changes in the effects of diffusion and chaos, the efficiency of the differential attack is very low and the attack is invalid. In order to verify the influence of a pixel change in the entire encrypted image, two measurement methods are commonly used: one is pixel change rate and the other is uniform average change intensity. Two encrypted images are represented by C_1 and C_2, respectively, only one pixel is different in their corresponding original images, and the gray values of images C_1 and C_2 at coordinates (i, j) are represented by $C_1(i, j)$ and $C_2(i, j)$, respectively.

$$D(i,j) = \begin{cases} D(i,j) = 0, & C_1(i,j) = C_2(i,j) \\ D(i,j) = 1, & C_1(i,j) = C_2(i,j) \end{cases} \tag{24}$$

The pixel change rate ($NPCR$) is defined as

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\% \tag{25}$$

In the formula, M is width and N is height of images $C1$ and $C2$. The meaning of $NPCR$ is to calculate the percentage of different pixels in two images. The uniform average change intensity $UACI$ is defined as

$$UACI = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C_1(i,j) - C_1(i,j)|}{255 \times M \times N} \times 100\% \tag{26}$$

From Table 2, we can know that the information entropy of the original image is equal to 6; the entropy of the traditional Hill encryption image is about 6. It is shown that the traditional Hill encryption algorithm does not make a significant change in the probability of the random distribution of the image, and there is no more agreement on the gray distribution. Information entropy is more small that the image is more orderly and the probability of the image random distribution is more small. Using the improved encryption algorithm to encrypt image, the information entropy is increased from the original data to 8, the information entropy is more great, random distribution of the image is more ideal, the more consistent in the gray distribution and the encryption effect is more ideal. From the pixel change rate, we can learn that the results of the improved algorithm are more large than the traditional Hill algorithm on the numerical value, and the results of the uniform average change intensity have a little difference [19].

6. Conclusion

In this paper, the tool used in this experiment is Visual Studio 2015, using the *c#.NET* language. We introduced the video monitoring system of the USV and the module of the system briefly, aiming at the favorable security and efficient efficiency of traditional image encryption technology; an improved algorithm is proposed based on Hill encryption algorithm. The algorithm is that a $m \times m$ self-invertible matrix is generated as the key matrix of this algorithm, then dividing the original image into $m \times m$ block image. The ith pixels of each image block will be grouped together and make up a temporary $m \times m$ image block, it is convenient for future encryption operation [20–23]. The temporary image matrix is encrypted with the key matrix A, transposing the encryption image matrix and double- layer encrypting the matrix and putting the obtained matrix into the ith position of the final encryption matrix. We use double-layer encryption strategy to decide the degree of scrambling and enhance the security of the encryption system. Results of experiments show that the algorithm has high efficiency of scrambling and the disorderly effect is uniform and the correlation of adjacent pixels is small, which changes the statistical information of the image and that is more ideal in the random distribution of the image and gray level. Through the analysis of its performance theory and experimental results, it has been shown that the improved algorithm is more successful than traditional Hill encryption algorithm and has great developmental potentialities. From the influence of pixel change rate and uniform average change intensity of encrypted image, the algorithm has not greatly improved the pixel change rate and value is too small that does not reach more than 0.9, they can improve by changing the length and width of the image. Therefore, considering the improvement in these two aspects will be a direction for the future.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by Research Project for FY2017 of International Association of Maritime Universities, China Postdoctoral Science Foundation under Grant 2015T80238, Natural Science Foundation of China under Grants 61771086 and 61401057, the Military Commission Equipment for the 13th Five-Year Field Fund Project under Grant 61403120402, Dalian Outstanding Young Science and Technology Talents Foundation, Natural Science Foundation of Liaoning Province under Grant 201602083, Science and Technology Research Program of Liaoning under Grant L2014213, Dalian Science and Technology Project under

Grant 2015A11GX018, Research Funds for the Central Universities 3132018144, 017180327, and 01760325, and Dalian High-level Innovative Talent Project under Grant 2016RQ035.

References

[1] K. Mani and R. Mahendran, "Generation of Key Matrix for Hill Cipher Encryption Using Classical Cipher," in *Proceedings of the 2nd World Congress on Computing and Communication Technologies, WCCCT 2017*, pp. 15–64, February 2017.

[2] M. Lakhera, M. M. S. Rauthan, and A. Agarwal, "Securing biometric template using double hill cipher with self-invertible key and random permutation of pixels locations," in *Proceedings of the 2nd IEEE International Conference on Next Generation Computing Technologies, NGCT 2016*, pp. 814–817, India, October 2016.

[3] A. N. Borodzhieva, "MS excel-based application for encryption and decryption of English texts with the hill cipher on the basis of 3×3-matrix," in *Proceedings of the 25th International Scientific Conference Electronics, ET 2016*, Bulgaria, September 2016.

[4] J. Zou and T. Weng, "A new image encryption instant communication method based on matrix transformation," *Smart Innovation, Systems and Technologies*, vol. 63, pp. 321–329, 2017.

[5] D. Xu, R. Wang, and Y. Q. Shi, "An improved scheme for data hiding in encrypted H.264/AVC videos," *Journal of Visual Communication and Image Representation*, 2015.

[6] T. Iakymchuk, A. Rosado-Munoz, M. B. Mompean, J. V. F. Villora, and E. O. Osimiry, "Versatile Direct and Transpose Matrix Multiplication with Chained Operations: An Optimized Architecture Using Circulant Matrices," *IEEE Transactions on Computers*, vol. 65, no. 11, pp. 3470–3479, 2016.

[7] M. Haj and M. Qatawneh, "Parallel Hill Cipher Encryption Algorithm," *International Journal of Computer Applications*, vol. 179, no. 19, pp. 16–24, 2018.

[8] T. Sivakumar and R. Venkatesan, "A novel image encryption approach using matrix reordering," *WSEAS Transactions on Computers*, vol. 12, no. 11, pp. 407–418, 2013.

[9] X. Liu, Z. Wei, and C. J. Carter, A novel image encryption approach using block based transformation and random phase encoding,.

[10] S. Muttoo, D. Aggarwal, and B. Ahuja, "A Secure Image Encryption Algorithm Based on Hill Cipher System," *Bulletin of Electrical Engineering and Informatics*, vol. 1, no. 1, 2012.

[11] M. A. Aljanabi, N. A. Shnain, and S. F. Lu, "An image similarity measure based on joint histogram — Entropy for face recognition," in *Proceedings of the 3rd IEEE International Conference on Computer and Communications (ICCC '17)*, pp. 1626–1631, Chengdu, December 2017.

[12] L. J. Ontanon-Garcia, M. Garcia-Martinez, E. Campos-Canton, and S. Celikovsky, "Grayscale image encryption using a hyperchaotic unstable dissipative system," in *Proceedings of the 2013 8th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 503–507, London, United Kingdom, December 2013.

[13] F. Gmira, S. Hraoui, W. Sabbar, and A. Jarrar Oulidi, "Image transaction encryption based on a dynamic upswing of hill cipher and JPEG compression," *International Journal of Imaging and Robotics*, vol. 17, no. 3, pp. 14–17, 2017.

[14] Cellular-news, "Maritime WiMAX Network Launched in Singapore," http://www.cellular-news.com/story/29749.php.

[15] M. G. V. Prasad and P. Sundarayya, "Generalized self-invertiblekey generation algorithm by using reflection matrix in hill cipher and affine hill cipher," in *Proceedings of the IEEE Symposium Series on Computational Intelligence*, vol. 8, pp. 11–23, 2018.

[16] R. Huang and C. Lu, "Research of H.264 video transmission encryption technology based on blowfish algorithm," in *Proceedings of the 4th International Conference on Computer Science and Network Technology, ICCSNT 2015*, pp. 931–935, China, December 2015.

[17] S. S. Giradkar and A. Bhattacharya, "Securing compressed video streams using RC4 encryption scheme," in *Proceedings of the Global Conference on Communication Technologies, GCCT 2015*, pp. 640–644, India, April 2015.

[18] R. Bhardwaj, "Enhanced encrypted reversible data hiding algorithm with minimum distortion through homomorphic encryption," *Journal of Electronic Imaging*, vol. 27, no. 02, p. 1, 2018.

[19] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4265–4276, 2015.

[20] D. Chen, N. Zhang, Z. Qin et al., "S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2017.

[21] J. Wu, K. Ota, M. Dong, J. Li, and H. Wang, "Big Data Analysis-Based Security Situational Awareness for Smart Grid," *IEEE Transactions on Big Data*, vol. 4, no. 3, pp. 408–417, 2018.

[22] L. Kuang, L. T. Yang, J. Feng, and M. Dong, "Secure Tensor Decomposition Using Fully Homomorphic Encryption Scheme," *IEEE Transactions on Cloud Computing*, vol. 6, no. 3, pp. 868–878, 2018.

[23] M. Tao, K. Ota, M. Dong, and Z. Qian, "AccessAuth: Capacity-aware security access authentication in federated-IoT-enabled V2G networks," *Journal of Parallel and Distributed Computing*, 2017.