Hindawi
Journal of Computer Networks and Communications
Volume 2019, Article ID 9629381, 14 pages
https://doi.org/10.1155/2019/9629381

Review Article

Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review

Sufian Hameed,[1] **Faraz Idris Khan**,[1] **and Bilal Hameed**[2]

[1]*IT Security Lab, Department of Computer Science, National University of Computer and Emerging Sciences (NUCES), Karachi, Pakistan*
[2]*Department of Computer Science, Bahria University, Karachi, Pakistan*

Correspondence should be addressed to Sufian Hameed; sufian.hameed@nu.edu.pk

Received 31 August 2018; Revised 14 November 2018; Accepted 4 December 2018; Published 10 January 2019

Academic Editor: Djamel F. H. Sadok

Copyright © 2019 Sufian Hameed et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Internet of things (IoT) is realized by the idea of free flow of information amongst various low-power embedded devices that use the Internet to communicate with one another. It is predicted that the IoT will be widely deployed and will find applicability in various domains of life. Demands of IoT have lately attracted huge attention, and organizations are excited about the business value of the data that will be generated by deploying such networks. On the contrary, IoT has various security and privacy concerns for the end users that limit its proliferation. In this paper, we have identified, categorized, and discussed various security challenges and state-of-the-art efforts to resolve these challenges.

1. Introduction

The emerging trends in embedded technologies and the Internet have enabled objects surrounding us to be interconnected with each other. We envision a future where IoT devices will be invisibly embedded in the environment around us and would be generating an enormous amount of data. These data would have to be saved and processed to make it understandable and useful.

An IoT model involves numerous actors which include mobile operators, software developers, access technology providers, and so on. The application domains of IoT are also very broad and such networks can be deployed in manufacturing, utility management, agriculture, and healthcare. IoT can be seen as the next generation interconnection paradigm which will enable connectivity among people's devices and machines enabling actions to happen without human intervention. The success of the IoT world requires a merger of a different communication infrastructure. This has lead to the design of smart gateways to connect IoT devices with the traditional Internet. Most recent efforts are directed to interconnect IoT infrastructure and cloud computing which supplements the potentials of IoT.

Increasing complexity of IoT networks also magnifies the security challenges faced by such networks. The complexity of IoT networks is attributed to the huge amount of devices connected to the Internet along with huge data generated by these devices. Attacks in IoT are possible as the devices in the IoT network are an easy target for intrusion [1]. Once compromised, the hackers can gain control and carry out malicious activities and attack other devices close to the compromised node. IoT devices do not have virus protection or malware protection software. This is a natural consequence of the low-memory and low-power nature of these devices. The unavailability of virus and malware protection on IoT devices makes them highly susceptible to become bots and carry out malicious activity to other devices in the network. Once an IoT device is hacked, the attacker can also hijack the routing and forwarding operations of the device. In addition to attacking various other devices in the network, attackers can also gain access to sensitive data collected and transmitted by the IoT devices. This lack of confidentiality, integrity, and security of data in IoT has the potential to disrupt the widespread adoption of this technology [2]. It is obvious from the discussion till now that the problem of securing IoT devices is immensely aggravated due to their

resource-constrained nature, due to which solutions for attack mitigation and privacy protection used on traditional networks cannot be readily deployed on IoT networks.

In this paper, we have discussed the state-of-the-art efforts to secure IoT networks and applications from the attacks and vulnerabilities briefly highlighted above. The IoT security challenges mainly fall under privacy in IoT, lightweight cryptographic framework for IoT, secure routing and forwarding in IoT, robustness and resilience management in IoT and DoS, and insider attack detection in IoT. Furthermore, we have identified and discussed open issues and challenges in each of the domains mentioned above.

The rest of the paper is organized as follows. Section 2 discusses privacy issues in IoT. In Section 3, state-of-the-art lightweight cryptographic framework for IoT is discussed. Section 4 discusses all the state-of-the-art proposals in secure routing and forwarding for IoT. State of the art in provisioning resilience and robustness management in IoT are discussed in Section 5. Section 6 summarizes state of the art in proposed denial of service and insider detection in IoT. We conclude our paper in section 7.

2. Privacy in IoT

2.1. Motivation. Privacy in IoT is a prime security issue that needs full attention from researchers in academia and industry. There is a dire need to propose protocols and management frameworks to handle privacy in IoT. IoT has become an integral part in various applications like remote patient monitoring, energy consumption control, traffic control, and smart parking system. In all of these applications, users require protection of personal information which is related to their movement, habits, and interactions with other people.

2.2. Challenges. With regards to privacy in IoT, every solution or framework must address the following challenges:

(1) *Profiling and Tracking*. Association of an identity with a certain individual is a threat as this may lead to profiling and tracking. Hence, one of the major challenges is to disallow such activity in IoT and take some preventive measures.

(2) *Localization and Tracking*. Localization is another threat as systems try to determine and record person's location through time and space. One of the major challenges of security solutions for IoT is to design protocols for interactions with IoT that discourages such activity. Profiling information related to a certain individual to infer interests by correlation between other profiles and data is very common in e-commerce applications. Huge challenge lies in balancing interests of businesses for profiling and data analysis with user's privacy requirements.

(3) *Secure Data Transmission*. Yet another security is to ensure that data are transmitted in a secure manner through the public medium without concealing information to anyone and thereby prevent unauthorized collection of information about things and people.

2.3. Existing Solution and Discussion. In this section, we discuss existing efforts in the direction of ensuring privacy in IoT application especially body sensor networks.

Most recent work which addresses the security and privacy challenges of cloud-based IoT can be found in [3]. Security and privacy requirements in cloud-based IoT as identified by the authors are identity privacy, location privacy, node compromise attack, layer removing/adding attack, forward and backward security, and semitrusted and malicious cloud security. Another recent work that is an attempt to analyze existing privacy-preserving solutions can be found in [4]. The authors identified the gaps in various proposals and put forward suggestions to remove them.

The authors in [5] surveyed existing IoT applications. In this work, the authors proposed a translation of their modules in a common system model and at the same time identified and studied differentiating behavioral pattern of sensor data generated. From the analysis, it was disclosed that almost all applications gather location and time information. Whatever data that are gathered can be of various types including video and audio. The authors surveyed up to date privacy countermeasures. Furthermore, potential threats to user privacy in participatory sensing which results from uncontrolled disclosure of personal information to untrusted people have been discussed. Also, the authors mapped their analysis to a proposed common system model for analyzing security in mobile participatory sensing application.

A detailed discussion on security threats and privacy in IoT architectures can be found in [6]. The discussion begins with detail layered architecture of IoT. Privacy and security threats at each level of the architecture are analyzed in detail. State of the art in presenting threat scenarios at various levels of the IoT architecture is discussed in detail. Based on the scenarios discussed, the security issues of importance are eavesdropping, man-in-the-middle and other similar attacks that jeopardize the data confidentiality and integrity, and grabbing control of some components. Along with that the authors also study the emerging EU legislation for IoT. It is important to understand the management domains of the IoT architecture. EU legislation requires an individual should be able to control his or her information at all levels of architecture. Issues of further study require an in-depth study of how this kind of control is technically supported. Energy aspects of privacy and threats require more in-depth study.

In [7], the authors surveyed privacy enhancements in IoT in various application domains. Key future security requirements for smart home systems are discussed. Also, the authors suggested a suitable security architecture for IoT. The gateway architecture is nominated to be the most appropriate for resource-constrained devices and for high system availability. This architecture implements sophisticated management algorithms on a reasonably powerful processor and can operate critical smart home functions. Apart from gateway architecture, other architectures are scrutinized for IoT are middleware architecture and cloud

architecture. Two technologies are discussed for a gateway architecture for assisting auto management: firstly, auto-configuration support enhancing system security and, secondly, automatic update of system software and firmware to maintain ongoing secure system operation.

Efforts in managing privacy for IoT by efficient data tagging through IFC (information flow control) tags can be found in [8]. The sensed data are tagged with privacy properties that allow trusted control access based on sensitivity. Due to the resource requirement of IoT, tagging is very expensive, and this work discusses the concerns about tagging resource-constrained IoT. Four properties of privacy-sensitive IoT applications including physical interaction, sensing valuable data, distributed implementation, and vulnerable sensors are illuminated which makes IFC data tag feasible for privacy preservation. Apart from these four, there are two more properties of such applications that are connected operation and skewed tag use that make implementation of IFC data tags much easier.

In [9], security challenges in mobile ad hoc networks are discussed in detail. There are various challenges to security design such as open peer to peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Considering these challenges building a multifence security solution that achieves both broad protection and desirable network performance is possible. Security issues and state-of-the-art proposals related to the multihop delivery of packets among mobile nodes are discussed. For a comprehensive security solution, it should span both layers and encompass all three security components of prevention, detection, and reaction.

Enabling technologies for IoT privacy provisioning such as RFID can be found in [10] with detailed discussion on threat analysis of RFID system components. RFID technology is considered good for tracking and keeping stock of items. In order to apply this to humans, there have to be laws and regulation to operate, and strict imposition to ensure acceptance as it can be abused. The authors conclude, in order to use RFID to enable IoT, issues with technological and social problems have to be resolved.

In [11], authors have proposed a Host Identity Protocol (HIP) and Multimedia Internet Keying protocol enabling secure network alliance with the network in a secure manner along with managing keys using a key management mechanism. HIP leverages public key cryptography to provide distinct identification of the IoT devices. Furthermore, the authors have extended HIP to have key management support.

Medical sensor networks (MSNs) require efficient and reliable access control that is a crucial requirement to authorizing staff to access private medical data and ensure productive and dependable access control. The authors in [12] have proposed an access control system enabling control on access in well-defined medical situations. The proposed system is an extension of the modular traditional role-based access control model. Modular design enables a simpler way of making a decision for access control and effective distribution of access control policies.

In [13], the authors proposed a privacy protection mechanism based on a concept of path jumbling which is a collective privacy-preserving mechanism. With the proposed mechanism, a user's privacy is preserved in a redistributed fashion by exchanging sensor readings.

The authors in [14] proposed a detailed analysis of threats related to privacy challenges in the IoT. Detailed analysis of seven threat categories identified by the authors is discussed. These seven categories are a) identification, b) localization and tracking, c) profiling, d) privacy violation interaction and presentation, e) life-cycle transitions, f) inventory attack, and g) linkage. Identification is a threat of attaching a (persistent) identifier with an individual and data about him. Location and tracking is the threat of determining and recording a person's location through time and space. Profiling is a threat of compiling information of individuals that infers interests by correlating with other profiles and data. Privacy violating interaction is a threat of conveying private information by a public medium and disclosing it to an unwanted audience. Changes of control sphere during lifecycle transition threaten privacy as smart things disclose private information. Unauthorized collection of information about the existence and characteristics of personal things is called inventory attack. In addition, another privacy threat is associated with combining and aggregating data from different data sources which often happen in IoT application. This will reveal information from a single data source that is not intended to be made public when its data were isolated. The authors conclude that profiling remains one of the severe threats that needs attention from the research community. The authors discuss two core thoughts: firstly, IoT is evolving which makes privacy a constant challenge and, secondly, a comprehensive framework is required, which caters threats identified by the authors.

In [15], authors have discussed the security of mobile sensing application. In this work, the authors presented nominated application scenarios in order to spotlight potential benefits inferred from their utilization. Authors studied heterogeneous statistics acquired by current mobile sensing applications and the flow of data in the application architectures. Particular emphasis is given on threats related to privacy. These threats are on primary information and sensor readings collected in existing mobile sensing deployments. These readings are spatiotemporal information, sound samples, pictures, videos, and accelerometer data. Temporal annotation of sensor data provides insights into the habits of the users that endanger privacy, and information in spatiotemporal readings itself threatens the privacy of the users. Automated recording of sound samples poses serious risks for user privacy in the absence of privacy-preserving mechanisms as confidential conversation can be recorded. Pictures and videos endanger the privacy of additional people captured in images by the user, as it may reveal their current location as well as the identity of social relations.

The authors in [16] have presented security architecture for IP-enabled IoT based on HIP (host identity protocol) and DTLS (Datagram Transport Layer Security) adapted to resource-constrained devices. In addition, authors propose key management architecture for IoT. Privacy protection is provided by proposing HIP-PSK (host identity protocol-preshared keys) and DTLS-PSK (Datagram Transport Layer

Security-preshared keys) that provide secure network access and communication.

In [17], the authors identified and discussed three representative sensing applications. They are personal sensing, designated sensing, and community sensing, each requiring heterogeneous security and privacy guarantees. Wireless community networks (WCNs) realize these sensing applications. WCN has emerged from the integration of wireless mesh networks, wireless sensor networks, and mobile communications that will form the future communication infrastructure for urban communities. Heterogeneous sensing applications have different security and privacy challenges. These security challenges are motivated by integration of sensors into WCN infrastructure. Such challenges are raised due to the presence of sensors in houses of community members or in mobile devices. The first challenge is to devise security and privacy model in order to understand exact risks and threats for each of application types. The second challenge is in personal and designated sensing applications. The access to measurements should be based on appropriate privacy-preserving access control mechanism. The third challenge is to devise mechanisms for privacy-preserving community sensing where the main concern is related to the anonymized sensed environmental data which could become public. Moreover, [18] proves to be useful in implementing privacy in sensing applications as suggested by the authors in [17].

In [19], the authors' categorized approaches in tackling IoT as rule-based and architectural-based approaches. They proposed an architecture-based privacy protection framework. IoT is modeled as cooperative distributed systems where things cooperate to attain individual or cooperative goals. Contract Net Protocol (CNP) is extended to support privacy protection for IoT.

Latest evaluations of IoT networks for security and privacy can be found in [20]. The authors focused on preserving privacy in home automation networks that are claimed to be extended to IoT applications. It is demonstrated that both basic cryptographic techniques and data manipulation are employed to save a user against a rival inside the IoT network or rival who have compromised remote servers.

A comprehensive survey of privacy and trust issues in IoT can be found in [21]. Traditional security countermeasures are quite different and cannot be applied immediately to IoT technologies due to heterogeneous standards and communication stacks involved. There is a desire for a flexible architecture to deal with hazards in a dynamic environment where scalability issues arise due to the high number of interconnected devices. The authors presented and discussed essential research challenges and prevailing solutions in IoT security, distinguishing open issues and proposing future directions for research. Besides, challenges in IoT is also discussed in [22] where authors introduced industrial IoT and discussed relevant security and privacy challenges and further give viable solutions which lead to a comprehensive security framework. More summarization of security threats and privacy concerns of IoT can be found in [23]. There are efforts in establishing a relation between information, privacy, and trust that can be found in [24].

In [22], analysis of security requirements, threat models, and security issues in IoT is discussed in detail with a comprehensive classification and taxonomy of attacks. Open problems and latest research issues are discussed in the paper. Possibilities for future research work are also discussed in the paper. The latest effort in classifying security in IoT can be found in [25]. The authors proposed a model based on privacy and classification called privacy information security classification (PISC). Privacy is divided into three security levels. Level 1 privacy is related to public information leakage of which will not cause serious consequences to the owner. Level 2 privacy is composed of anonymous and semianonymous personal data. Level 3 privacy is information directly corresponding to user's identity such as fingerprint, identification card information, and Internet protocol address. Forging of fingerprint leads to useful information getting lost or stolen. Therefore, complex security protection measures in protecting level 3 privacy information are required. Different security protection technologies are required to achieve different security goals for the different levels of privacy information.

The research community has proposed protocols for ensuring privacy in IoT; such as in [26], the authors proposed two sensor-based secure communication protocols for healthcare systems based on IoT. Latest work on key management protocol for IoT can be found in [27]. The protocol also performs robust key negotiation, lightweight node authentication, fast rekeying, and efficient protection against replay attacks. Proposed key management protocol (KMP) is integrated at layer 2 of the protocol stack. It leverages "fixed" elliptic-curve Diffie–Hellman (ECDH) exchange and the (elliptic curve) Qu-Vanstone implicit certificates. KMP is implemented in open source OpenWSN protocol stack. A comprehensive survey on secure communication protocols for IoT can be found in [28] where the authors have highlighted the inapplicability of traditional security protocols in IoT and gave a detailed taxonomy of key distribution and management protocols.

2.4. Open Issues and Future Directions. Some of the major open issues and/or future directions that are emerging in the domain of privacy for IoT are listed as follows:

(1) *Comprehensive Privacy-Preserving Frameworks*. In all the existing work that exists in the literature till now, there is no comprehensive framework that ensures privacy in IoT for a large class of applications. There is a dire need to have a generic lightweight cryptographic privacy-preserving algorithm that ensures confidential exchange of data at the same time anonymizing the origin of data.

(2) *Context-Aware Privacy Policies*. Latest trends in IoT privacy protection are user-centric and context-aware privacy policies. Along with them, other emerging techniques are context-centric and self-adaptive privacy-preserving mechanisms and protocols supporting ambient intelligence. One of the novel emerging fields is of privacy preservation of data

streams in IoT. This requires dynamic data access control mechanisms and data management policies.

(3) *Game Theory-Based Privacy-Preserving Incentives*. Game theory has lately been used to analyze location privacy. An interesting open research question is how to implement incentives in the IoT architecture's privacy-preserving protocols by utilizing game theory.

(4) *Network Virtualization and SDNs*. For the next generation networks, context management is expected to interact with underlying IoT technologies and deal with related privacy issues improving quality of the context. Hence, for the upcoming years, development of more sophisticated privacy models and practically relevant privacy-oriented security protocols and mechanisms are identified as the research direction of extreme importance. Network virtualization adaptation for preserving privacy for a huge amount of data being handled in IoT deployments and cloud management has emerged as a potential approach. Software defined networking (SDN) lately has emerged as a paradigm for network virtualization. Also, SDN regulates the network by centralizing the routing and forwarding functionality at a central point, which is known as the controller. This can help the network operator and administrator to implement privacy over the whole network. Initial architecture in this direction can be found in [29].

3. Lightweight Cryptographic Framework for IoT

3.1. Motivation. IoT introduces new challenges in terms of energy and power consumption. It is desired that the cryptographic primitives designed for IoT should be lightweight. These primitives must consume fewer resources without compromising the required level of security. Hence, the research community has started focusing on lightweight cryptography. Properties of lightweight cryptography are discussed in ISO/IEC 29192 and ISO/IEC JTC 1/SC 27. There is also a project of lightweight cryptography (ISO/IEC 29192) under the process of standardization. Lightweight cryptography in ISO/IEC 29192 is described based on the target platform. Chip size and energy consumption are important measures to assess lightweight properties. Furthermore, small code and/or RAM size are preferable for lightweight applications in case of software implementation.

3.2. Challenge. Given the constraints of hardware resources, there is a need to design a lightweight cryptographic framework for IoT. This can be achieved by proposing cryptographic primitives that need to be revisited and designed considering the constraints of IoT devices.

3.3. Existing Solution and Discussion. In this section, we discuss efforts in the direction of proposing a lightweight cryptographic framework for IoT.

The authors in [30] have proposed a security architecture that confirms the security goals discussed in the paper. Proposed solution works according to the lifetime of a smart object in IoT network. The keying material is managed by TTP infrastructure. The proposed framework is used to manufacture the smart objects in a protected manner.

In [18], the authors have proposed a resource friendly, fast and distributed security mechanism for key agreement, and verification of identification parameters in WSN. The proposed system is based on alpha secure polynomials that have been proposed for key distribution and establishment. The authors in [31] have proposed mechanisms to make the computation of polynomials more lightweight for IoT.

The authors in [32] have identified three devastating security compromise, initiated from the Internet, at the transport layer in opposition to the low power and lossy networks. The authors observe provisioning E2E security is not possible with ease due to a variety of usage scenarios like CoAP/CoAP (Constrained Application Protocol), DTLS/DTLS (Datagram Transport Layer Security), HTTP/CoAP, and TLS/DTLS which are arbitrated by 6LBR (6LoWPAN Border Router) having different constraints and requirements. Secure E2E connection only provisions secure communication channel, and LLNs (low-power and lossy networks) are still vulnerable to resource exhaustion, flooding, replay, and amplification attacks. The authors have discussed two approaches to mitigate such attacks. First, mapping TLS or DTLS protocol to ensure end-to-end security at application layer which disallows 6LBR to gain access to data in transit. Second, DTLS-DTLS tunnel is used to protect LLN.

Lightweight key predistribution schemes can be found in [33]. Such schemes are proposed for IoT. Improvement in resource efficiency of such algorithms is proposed in [30]. More efforts on optimization of the cryptographic operations in IoT security provisioning are proposed in [34] where the authors have shown the equivalence of the MMO problem to finding close vectors in a lattice. In [35], the authors proposed a new efficient ID-based key establishment scheme. The identity-based scheme consists of a node with an identifier and a trusted third party (TTP) which provides the node in the network with secret keying material linked to the device identifier in a secure way. Secret keying material and the identity of the other node are used by other nodes to generate a common pairwise key for secure communication. Scheme put forward by the authors is efficient in terms of key computation time. In [36], the authors have proposed a key management service for BSNs (body sensor networks). The key management service considers the resource inefficiency of IoT and low-power devices.

The authors in [37] have presented security challenges of IoT communication. Architectural design for secure IP-based IoT is reviewed by the authors. The lifecycle of an IoT device and its capabilities should be considered for designing a security architecture. The architectural design should include the aspects of trusted third party and type of protocols applied. As another requirement, an architecture should scale from small-scale ad hoc security domains to large-scale deployments. Lightweight protocols should be

adopted within the architecture. Another interesting point raised by the authors is related to the placement of security at different layers (link, network, or application layer) in IoT, as each layer has different security requirements and communication patterns. If security is provisioned at the application layer, then the network is open to attacks. However, focusing security on network or link layer introduces possible interapplication security threats.

Efforts in proposing a lightweight security framework can be found in [38] where the proposed architecture provides a holistic security approach which contains lightweight authentication and authorization functionality on constrained smart objects. In [39], the authors proposed a lightweight framework comprising of DTLS, CoAP, and 6LoWPAN protocols to provision end-to-end security for IoT. Efforts in evaluating the lightweight cryptographic framework can be found in [40], and the authors' proposed framework which assists the embedded software engineer for selecting best cipher to match requirements of an application. A lightweight framework to provide access control in IoT can be found in [41]. The authors proposed a generic authorization framework for IoT devices. Evaluation of the proposed framework is also discussed.

Standard compliant security framework can be found in [42], and the authors intend to make it applicable for future IoT paradigm. Another similar work that proposes an end-to-end security framework for IoT can be found in [43].

In [44], the authors proposed a security scheme for IoT based on established standards and prevailing Internet standards on a low-power hardware platform. Proposed security solution fails in preventing against routing attacks and is too heavy for low-power devices. Another effort in the evaluation of resource consumption during the provisioning of security services can be found in [13]. The work lacks a new proposal to deal with end-to-end security of IoT. The authors in [45] have evaluated secure communication mechanisms and compare them in terms of resource consumption. The work concludes with the best secure communication mechanism.

In [46], Hameed et al. proposed a security middleware for security weaknesses in NFC-based systems. The middleware in the initial stage is capable of detecting malicious NFC tags or smart posters with little effect on CPU and memory. The authors further extended their middleware with lightweight primitives to provide confidentiality and integrity support for arbitrary NFC applications [47, 48].

3.4. Open Issues and Future Directions. We have identified following shortcomings for potential future work directions in this area:

(1) *Focus on Frameworks Rather than Cryptographic Algorithms*. Most of the existing work has focused on optimizing the algorithmic steps in the cryptographic algorithms performing cryptographic operations. None of the current work considers the framework of protocols that perform lightweight operations to secure the IoT network. Security provisioning over IoT is very challenging as compared to WSN due to heterogeneous nature of devices. Furthermore, they are deployed in unattended environments that are closer to humans than WSN nodes. In contrast to WSN IoT is expected to have IPv6, UDP, and web support. Communication in IoT can be secured by (1) lightweight security protocols proposed for constrained environments, i.e., WSNs, (2) novel security protocols that meet the specific requirements of IoT, and (3) established security protocols which already exist on the Internet. The security protocols designed for WSN are not designed for the IP network. In order to use them, IoT requires modification of WSN protocols and their provisioning on the Internet. Due to a huge number of devices on the Internet, security solution requires modification that is not practical in the current Internet. The primary challenge that hinders applicability of Internet security solutions in IoT is that these solutions are not inherently designed for resource-constrained devices but for standard computing machines which have sufficient energy resources, processing capability, and storage space.

(2) *Utilization of SDNs for Lightweight Security Provisioning*. Apart from novel security solutions for IoT, emerging paradigm of SDN, with the potential of centralizing routing functionality, enables central monitoring and reconfiguration of the network. This opens new possibilities of implementing a lightweight cryptographic framework for IoT that runs light security protocols at the SDN controller. Most of the major cryptographic functionalities are concentrated at the central controller. Hence, heavy cryptographic operations are offloaded to the central SDN controller that communicates with the IoT nodes.

4. Secure Routing and Forwarding in IoT

4.1. Motivation. IP-based IoT inherits attack threats of IPv4. Some of these well-known attacks are black-hole attacks, sybil, spoofing, smurfing, eavesdropping, neighbor discovery, man-in-the-middle, rogue devices, and fragmentation attacks. This means IoT is in need of the same security measures as required for IPv4, as it is envisioned with IoT that the physical world will be connected with the Internet which leads to a wide variety of security concerns. Attack threats not only include manipulation of information but actual control of devices in IoT network. With more electronic systems, i.e., Modbus, SCADA becoming part of IP-based systems, a significant increase in attacks are expected. This adds new security threats as heterogeneous devices become part of the IoT network.

In a wireless mobile network, a route is established when route information is transmitted from node to node until the destination is found. Throughout this route maintenance phase, nodes are added or deleted. Furthermore, these nodes may unnecessarily delay transmission of control information, which usually is done by selfish or misbehaving nodes. During this phase of route setup and discovery, several attacks are possible by malicious nodes in routing

information. For example, a certain node may introduce a routing table overflow attack by transmitting a huge amount of false route information to neighboring nodes which cause the neighbor's routing table to overflow. Due to such actions, the table is filled with spurious routes and real routes are denied to occupy the routing table.

4.2. Challenges. The key challenges in secure routing and forwarding are highlighted below:

(1) *Secure Route Establishment*. One of the key challenges is to establish secure routing protocol for data transmission in IoT. Such a protocol should be able to securely establish a route and guarantee secure route among communicating nodes. The computations performed for the purpose of routing data should be lightweight in order to be adequately served by the low-powered IoT networks.

(2) *Isolation of Malicious Nodes*. Another challenge is to quickly and robustly detect malicious nodes and design techniques to isolate them from the IoT networks. The protocol should be able to isolate misbehaving nodes in the network so that disruption in the routing process is minimized or eliminated altogether. Current routing protocols for IoT are insecure as most IoT networks are self-organizing and usually operate without any human involvement. Hence, malicious nodes can be introduced in the IoT network with relative ease, so there is a need to design a protocol that has methods and techniques to block malicious nodes from joining the network or detect them as soon as they start malicious activities.

(3) *Self-Stabilization of the Security Protocol*. The protocol should self-stabilize which means it should be able to recover automatically from any kind of problem within a certain time without human involvement.

(4) *Preservation of Location Privacy*. Location privacy should be maintained for the IoT devices in the IoT network. Hence, for a secure routing protocol, it should be able to maintain location privacy.

4.3. Existing Solution and Discussion. In this section, we discuss efforts in the direction of secure routing and forwarding in IoT.

IoT not only requires provisioning of security services but often experiences problems in routing and forwarding the data. Securing a routing algorithm for IoT has become a crucial requirement. A comprehensive state of the art in securing routing for WSN can be found in [49]. The authors proposed a schematic taxonomy of key design issues in WSN routing protocols and defined the design categorization factors for secure routing, i.e., basic, essential, and optional. Also, a comparative study is performed on the basis of key design attributes, security objectives, and attacks prevention which considered recent advancements in the area of secure WSN routing. Security aware routing protocols for ad hoc networks can be found in [50]. The authors developed a generalized framework with open feedback and explicit representation of attributes and choices. With this, users can adapt the security attributes in runtime and talk terms for alternative routes which are calculated on the basis of cost-benefit analysis of the performance penalties against offered protection in the scenario.

In [51], the authors have proposed an adaptive, flexible, and lightweight scheme for the protection of integrity and reauthentication based on hash chains which is often called as ALPHA. The proposed scheme enabled hop by hop and end-to-end integrity protection for multihop wireless networks. End-to-end integrity protection which is based on secret sharing will be replaced which cannot be authenticated by relays.

The authors in [52] proposed a secure and efficient cost assurance routing protocol for IoT (CASER). Routing in CASER is based on geography and do not rely on flooding to broadcast routing information in the network. It balances energy consumption and increases network lifetime. Furthermore, it sends messages by two routing strategies random walking and deterministic routing. Distribution of two strategies is decided by particular security requirements. The selection of two strategies is probabilistically controlled by assigning a probability to a variable representing the security requirement that is dependent on the cost factor of the route. The authors presented a quantitative security analysis of CASER. No software or component architectural details of CASER are discussed.

Advance security attacks in routing can be found in [53]; the authors consider node capture attack where the attacker captures a legitimate node, and by extracting cryptographic keys, it makes the captured node as malicious ones which run the malicious code. To attract the traffic, the compromised node broadcast a fake RREQ with a false hop count.

Secure multihop routing for IoT is proposed in [54], where multilayer parameters are embedded into the routing algorithm. It was shown by the authors that the proposed algorithm is suitable for IoT communication.

There are several efforts where researchers have proposed trust-aware routing algorithms such as in [55] where authors claim to propose routing framework that has the attribute of lightweight and has high ability to resist various attacks. In [56], the authors proposed secure procedures for resource insufficient IoT devices. Comprehensive analysis of security capabilities of IoT can be found in [57], and the analysis is performed by implementing and demonstrating famous routing attacks launched in 6LoWPAN network running RPL. Another work that gives a detailed survey on security issues in IoT can be found in [58]. The authors discussed security measures that are adopted at heterogeneous layers of the IoT architecture.

Other such efforts in proposing a secure routing algorithm for IoT can be found in [9, 59–62]. In all of these works, the authors have proposed a trust-aware secure routing algorithm for IoT. Detecting routing attacks in sensor networks using the intrusion detection system can be found in [63]. The abnormal traffic behavior is detected

using clustering algorithms that construct a model for normal traffic and conclude with abnormal traffic behavior.

In addition to efforts in secure routing, there are proposals of detecting devastating attacks in IoT routing; such as in [64], an intrusion detection system to distinguish sinkhole attacks on the IoT routing services is proposed. Experimental evaluations show the effectiveness of the proposed idea.

4.4. Open Issues and Future Directions. We have identified following shortcomings for potential future work directions in this area:

(1) *IoT Network Performance-Focused Routing Protocol Design*. Although there are various efforts which have dealt with the problem of secure routing and forwarding, none of the work has considered the performance of the IoT network when secure routing mechanisms are incorporated. There are complex mechanisms such as the one that proposed IDS to detect attacks in the network. Such mechanisms do not consider the resource limitation of IoT devices. However, lightweight IDS may help us in detecting malicious activities in IoT network and mitigate routing attacks with IoT network. Novel designing of a lightweight IDS requires attention from the networking research community.

(2) *Effective and Fine-Grained Control over Routing Activities*. Apart from lightweight IDS for IoT, regulating the IoT network from a central point can help us in monitoring the state of the whole network. In addition to this, we also need fine-grained security and routing control policies that can be changed quickly to respond to security threats. Paradigms such as SDN, which centralizes the control plane at the controller, can help us in routing the data securely in the IoT network. Hence, novel security solutions over SDN are required which route and forward IoT network data by preserving their integrity.

5. Robustness and Resilience Management in IoT

5.1. Motivation. IoT network constitutes heterogeneous devices where managing such kind of network is not an easy task. Lately, researchers have focused their attention towards service-oriented architecture (SOA) for the management of IoT [65], as it caters the integration and management of diverse services. With the use of such a paradigm, a lightweight middleware can be constructed upon IoT devices providing an abstraction of integratable and manageable IoT services. Developers and users of IoT devices are free of details on what and how devices are used and connected. Faults in IoT applications are not tolerable, as system failures may disrupt user's everyday activities or even lead to danger in lives. To worsen the situation, SOA is prone to all the faults related to distributed systems [66]. Hence, SOA-based middleware for IoT is subjected to all the inherent problems of distributed systems. Besides normal faults in IoT devices, such faults may occur due to DoS attacks on IoT devices and services disrupting IoT services to the application users.

5.2. Challenges. The key challenges in robustness and resilience management are highlighted below:

(1) *Attack Tolerance*. IoT networks need new and novel network designs that are inherently tolerant to intrusions and other malicious attacks.

(2) *Early Detection of Attacks*. Once an attack has been initiated, the IoT network must have methods and protocols to ensure that the attack is detected as quickly as possible before the attack causes major damage and spreads out across the network.

(3) *Quick Recovery from Failures*. Timely recovery from failures becomes critical in the IoT network. Prolong disruption in IoT services may lead to a life-threatening situation especially for disaster management applications. Hence, it is required that the resource management middleware designed for IoT network should timely detect failures and resolve the situation. There are various possible solutions to resolve IoT device failures. One of the possible solutions is to replicate resources [67] and deploy them in the same environment. This solution is costly, as it requires duplication of resources.

5.3. Existing Solution and Discussion. In this section, we discuss efforts in the direction of ensuring robustness in IoT network.

In [68], the authors addressed the problem of a misbehaving node in the network. They proposed a preliminary description of protocol ECoSec (Efficient Cooperative Security) which controls the admission and revocation of nodes by collaborating with other nodes by two voting procedures. Trust management is also looked upon by the researchers to provide resilience in IoT. In [69], the authors have analyzed the proposed protocol ECoSec (Efficient Cooperative Security) operation and parameters for node agreement that is performed for admission voting and revocation information. Other work on handling such issues by context awareness and intelligence can be found in [70, 71]. In [72], the authors discussed resilience management in IoT. AI-based approaches to provide fault tolerance in IoT can be found in [73] where the authors proposed hybrid cross-layer and fault-tolerant routing protocol based on learning automata. The algorithm dynamically adapts to the dynamic environment and then chooses an optimal action. Also, the algorithm adopts fault-tolerant routing which is energy aware. Energy is conserved by the sleep algorithm that is coordinated by a dynamic and adaptive scheduling algorithm.

Efforts in fault management can be found in [74] where authors put forward a fault management structure that is layered for diverse IoT networks. In order to realize efficient end-to-end transmission, fault detection and location fuzzy cognitive maps theory is introduced. The authors do not evaluate the overhead of the layered architecture. In [75],

distributed fault tolerance is developed and implemented which will configure itself based on user policy and requirements. Overhead of incorporating middleware and framework for IoT and M2M is not discussed in this work. Furthermore, the effectiveness of the distributed mechanism as compared to the centralized approach is also not discussed by the authors.

In another work [76], a self-learning-based sensor fault detection for monitoring industrial IoT is put forward by the authors. Responsiveness of the self-learning module is not evaluated and discussed. In [77], the authors proposed a network management framework for WSN, which is self-optimizing and fault tolerant. The cost associated with message passing middleware is not discussed in this work. Researchers have considered cloud-computing frameworks to provide fault tolerance to WSN such as in [78]. Evaluation of configuring failures in a sensor network is not discussed in this work as well. A similar effort can be found in [79] where the authors present a cloud-based framework to evaluate failures in a sensor network.

In [80], the authors propose network management protocol for WSN to manage failures in the network. Similarly, in [81], the authors proposed a novel architecture for scalability and fault tolerance in healthcare. Fault tolerance is attained by backup routing between nodes. Other such work related to managing WSN can be found in [82]. More work on the management of M2M can be found in [83] where minimum requirements for M2M network management are presented along with standardization activities.

5.4. Open Issues and Future Directions. People have approached the problem of ensuring robustness in IoT network by proposing protocols and network management framework. Faults in IoT network can occur due to either network attacks or depletion of energy. Efforts in tackling faults are numerous, and most of them have not considered the resource constraint nature of IoT devices. Centralizing the network view can ensure failures over IoT network to be controlled and provision fault-tolerant routing. As the decisions of routing will be concentrated on the controller, it will be possible to detect faults centrally. By detecting faults, decisions to divert the traffic to an alternative server or path will be carried out at the controller. Creative solutions that detect faults in a timely manner are required so that actions can be taken promptly to handle the situation by suggesting alternate possibilities.

6. Denial of Service and Insider Attack Detection in IoT

6.1. Motivation. Denial of service (DoS) attacks have devastating effects on IoT applications [84]. In IoT applications, availability of IoT service and devices is an important factor. DoS attacks make the IoT services unavailable, thus disrupting their normal operations. DDoS attacks are normally launched in a coordinated manner from multiple attackers at the same time, and their detection before the services become unavailable is quite difficult.

With IoT becoming an integral part of business applications. Businesses face a remarkable challenge of understanding and addressing risks of protecting themselves from a range of insider attacks. These attacks are usually launched by the use of devices that are unknown and remain undetectable and unmanaged by the IoT applications.

6.2. Challenges. The key challenges in DoS and insider attacks are highlighted below:

(1) *Resource Efficient DoS Attack Detection*. As DoS attacks are difficult to detect before the attack is launched, efficient DoS detection solutions are required. There exist various proposals where DDoS is dealt for traditional Internet such as in [85]. Detection of DDoS in IoT is a challenging issue as IoT network and traffic characteristics are quite different from the traditional network. Due to the limitation of IoT devices, resource-efficient DDoS detection and countermeasure techniques are required. Such techniques can be centralized such that based on monitoring the traffic in the IoT network centrally. Certain probabilistic techniques can help us in inferring the possibility of DDoS attacks. On the contrary, such techniques can be distributed where multiple IoT devices collaboratively infer the possibility of a DDoS attack in IoT network.

(2) *Resource Efficient Countermeasures*. Once a DoS attack is detected, there is a need to deploy countermeasures to mitigate the attack. Since IoT networks are extremely resource constraint, there is a need to design lightweight and energy efficient countermeasure strategies.

(3) *Resource Efficient Insider Attack Detection*. In order to prevent insider attacks in IoT, it is required to authorize IoT nodes becoming part of the IoT network. Techniques for detecting insiders in IoT network should be efficient and react in a timely manner. Otherwise, a devastating situation may arise as these insiders may leak confidential data by compromising nodes within the network or disrupt the operation of the IoT network by launching attacks such as DDoS attacks.

6.3. Existing Solution and Discussion. In this section, we discuss efforts in countering DDoS and insider attacks in IoT.

Insider attacks have received attention from researchers such as in [86]; the authors proposed a mechanism that manages the network using a node, which monitors the network constantly. The proposed algorithm works by maintaining a dynamic threshold. The threshold is adjusted by the view of overall packet loss situation in real time. This results in a decrease in the detection rate due to loss associated with the false alarm. The authors proposed a trust mechanism based secure routing protocol in [87]. The proposed algorithm investigates neighborhood activities based on the mechanism of spatial correlation and requires no knowledge of malicious sensor. It is important as the

prehand knowledge of sensor causes excess training overhead and discusses a grave strain in which attack behaviors alter dynamically. In [88], the authors proposed a rule-based anomaly detection system called RADS. The proposed idea revolves around detecting sybil attacks in 802.15.4 like WSNs by monitoring.

Efforts addressing DDoS attacks in IoT are discussed as follows. In [89], the authors put forward a framework that can be spread out in an existing network and can prevent forged messages that are broadcasted in the entire network. The filters are used to actually verify fake messages. Some of the nodes in the network have high processing and battery power than the other nodes. The nodes are called as adjunct nodes that are used to monitor the state of the network and perform appropriate actions when required. The authors in [90] aim to save WSN from DDoS attack using a mechanism which utilizes profile for provisioning security against various attack. Sensor nodes monitor the surrounding environment and deliver acquired data to the sink node for profiling. Profile-based protection scheme (PPS) is used to supervise the activities performed in the network. A comprehensive taxonomy of DoS attacks in WSN can be found in [91]. The taxonomy identifies the attacker, attack victim, and vulnerabilities.

A detailed description of IDS for IoT i.e., SCADA can be found in [92], and it has briefly discussed the history of research in IDS techniques. 6LoWPAN-based IoT when subjected to denial of service attack often experiences devastating situation. In [93], the authors proposed DoS detection architecture for 6LoWPAN-based IoT. The authors do not evaluate the cost of communication among components of the proposed architecture and overhead. Moreover, being a centralized architecture, it is subjected to a single point of failure. Variants of broadcast protocol i.e., TESLA for IoT which is DoS tolerant can be found in [94].

In [95], the authors proposed an AI-based approach to counteract DDoS by proposing learning automata-based preventive scheme. SoA-based framework is used for IoT due to its huge potential for a large number of applications. A cross-layer model for DDoS mitigation is used. IoT is typically resource constraint hence communication among layers incurs a cost. The authors do not evaluate the effectiveness of the cross-layer model. Learning automata mechanism is heavy to implement which might not be feasible for a huge network with various types of IoT devices.

In [96], the authors proposed an IDS framework for IoT. Monitoring system and detection engine are the components of the proposed framework. Evaluation of the proposed architecture with the increasing size of 6LoWPAN is not discussed. Communication cost of IDS framework will increase with the increasing size of the 6LoWPAN. Latest work in IDS for IoT can be found in [97] where possible attacks in IoT is discussed and along with lacking in current IDS for IoT. Different categories of IDS for IoT are discussed, and various existing types of IDS for the conventional Internet are highlighted which are to be evaluated for the RPL network.

6.4. Open Issues and Future Directions. Most of the proposed frameworks for tackling DDoS and insider attacks are based on monitoring system and detection engine. Implementing a detection engine over IoT network is resource consuming as they are based on AI algorithms. Hence, novel lightweight solutions for detecting DoS attacks is required. Apart from novel lightweight solutions, emerging paradigm of SDN enables monitoring of network state from a central point called controller. By monitoring flows at the controller, it is possible to implement algorithms to detect DDoS attacks and malicious activities such as insider attack [29]. This will also offload the tasks of defeating DDoS attacks from IoT devices to resource sufficient device that hosts SDN controller possibly the gateway device connecting IoT devices. A good hybrid solution would be to integrate IoT gateways with emerging SDN-based solutions that are capable of efficiently detecting [98] and mitigating [99] DDoS in conventional IP networks (Table 1).

7. Conclusion

In this paper, we have categorized and discussed the state-of-the-art work done in ensuring security in the IoT network. Efforts in privacy provisioning, lightweight cryptographic framework, secure routing and forwarding, robustness and resilience management, denial of service, and insider attack detection are discussed comprehensively. Privacy is crucial in IoT especially as the characteristics of such a network is different than the typical Internet network. Such issues and requirements are identified and discussed in this paper. Besides privacy for ensuring security in the IoT network, lightweight cryptographic primitives are required which are suited for IoT network. All the efforts in this direction are compiled and future actions are discussed.

In order to preserve privacy, context-aware techniques and lightweight protocols are proposed and most lately virtualization techniques are used to maintain the integrity of the data. For lightweight cryptographic primitives, novel solutions are required which should consume limited resources of an IoT mote. Apart from that, SDN solution offers to implement lightweight cryptographic solutions over IoT with the assistance of centralized routing carried at the SDN controller. IoT network experiences failures due to IoT nodes being subjected to heterogeneous kind of network attacks. Efforts in this direction are discussed with future insight. Faulty nodes within the IoT network can be experienced due to denial of service attacks launched by multiple coordinated nodes. Furthermore, such faults are prevalent due to frequent insider attack within the IoT network. To realize fault tolerance in IoT, centralized monitoring of the network state is required in order to timely react to counter faulty nodes within the network. Virtualization technology like SDN offers to centralize monitoring of the network which can assist in suggesting alternative servers or path to ensure consistent provisioning of service. As far as DDoS in IoT is concerned, lightweight detection engine suitable for IoT is required to detect and mitigate DDoS in a timely

Table 1: Comparison of challenges and open/future issues for different security requirements in IoT network.

Security requirements	Challenges	Open issues and future directions
Privacy	Profiling and tracking Localization Secure data transmission	Comprehensive privacy-preserving frameworks Context-aware privacy policies Game theory based privacy-preserving incentives Network virtualization and SDNs
Confidentiality	Lightweight primitives Consume low resource	Efficient holistic frameworks Utilization of SDNs for lightweight security provisioning
Secure routing	Secure route establishment Isolation of malicious nodes Self-stabilization of the security protocol Preservation of location privacy	IoT network performance focused routing protocol design Effective and fine grained control over routing activities leveraging SDN
Robust and resilient management	Attack tolerance Early detection of attacks Quick recovery from failures	SDN-based centralized management frameworks
Attack detection (DDOS and insider)	Resource efficient DoS attack detection Resource efficient countermeasures Resource efficient insider attack detection	Lightweight solution for resource constraint device Centralized SDN detection and mitigation algorithms

manner. Centralized monitoring enabled by SDN can assist in detecting DDoS and mitigate them within an IoT network.

For all of the security requirements, there is a need for a centralized management framework which can provide all the discussed security issues and requirements within the IoT network. SDN is a hot candidate which provides central configuration of the network by the controller which manages the network. Initial efforts in this direction can be found in [29]. There are still a lot of opportunities and issues which need to be dealt with in order to realize a comprehensive centralized management framework for provisioning security over IoT. SDN needs to be studied thoroughly so that it can be customized to provide management services over IoT network.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] X. Xiaohui, "Study on security problems and key technologies of the internet of things," in *Proceedings of IEEE Fifth International Conference Computational and Information Sciences (ICCIS)*, Hubei, China, June 2013.

[2] A. Kanuparthi, K. Ramesh, and S. Addepalli, "Hardware and embedded security in the context of internet of things," in *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*, pp. 61–64, Berlin, Germany, November 2013.

[3] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[4] N. Aleisa and K. Renaud, "Privacy of the internet of things: a systematic literature review," in *Proceedings of 50th Hawaii International Conference on System Sciences*, Waikoloa, HI, USA, 2017.

[5] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," *Journal of Systems and Software*, vol. 84, no. 11, pp. 1928–1946, 2011.

[6] J. Veijalainen, D. Kozlov, and Y. Ali, "Security and privacy threats in IoT architectures," in *Proceedings of 7th International Conference on Body Area Networks*, Oslo, Norway, September 2012.

[7] H. Lin and N. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.

[8] D. Evans and D. M. Eyers, "Efficient data tagging for managing privacy in the internet of things," in *Proceedings of 2012 IEEE International Conference on Green Computing and Communications*, pp. 244–248, Besancon, France, November 2012.

[9] H. Yang, H. Luo, Y. Fan, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38–47, 2004.

[10] B. Khoo, "RFID as an enabler of the internet of things: issues of security and privacy," in *Proceedings of 4th International Conference on Cyber, Physical and Social Computing*, pp. 709–712, Dalian, China, 2011.

[11] F. V. Meca, J. H. Ziegeldorf, P. M. Sanchez, O. G. Morchon, S. S. Kumar, and S. L. Keoh, "HIP security architecture for the IP-based internet of things," in *Proceedings of IEEE Advanced Information Networking and Applications Workshops (WAINA)*, Barcelona, Spain, March 2013.

[12] O. Garcia-Morchon and K. Wehrle, "Modular context-aware access control for medical sensor networks," in *Proceedings of 15th ACM Symposium on Access Control Models and Technologies*, Pittsburgh, PA, USA, June 2010.

[13] D. Christin, A. Reinhardt, and M. Hollick, "On the efficiency of privacy-preserving path hiding for mobile sensing applications," in *Proceedings of IEEE LCN*, Sydney, NSW, Australia, 2013.

[14] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[15] S. Gutwirth, R. Leenes, P. De Hert, and Y. Poullet, *European Data Protection: Coming of age*, Springer Science & Business Media, Berlin, Germany, 2012.

[16] O. Garcia-Morchon, S. L. Keoh, S. Kumar, P. Moreno-Sanchez, F. Vidal-Meca, and J. H. Ziegeldorf, "Securing the IP-based internet of things with HIP and DTLS," in *Proceedings of Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Budapest, Hungary, April 2013.

[17] D. Christin, M. Hollick, and M. Manulis, "Security and privacy objectives for sensing applications in wireless community networks," in *Proceedings of ICCCN*, pp. 1–6, Zurich, Switzerland, August 2010.

[18] H.-C. Chen, "Secure multicast key protocol for electronic mail systems with providing perfect forward secrecy," *Security and Communication Networks*, vol. 6, no. 1, pp. 100–107, 2012.

[19] A. Samani, H. H. Ghenniwa, and A. Wahaishi, "Privacy in Internet of Things: a model and protection framework," *Procedia Computer Science*, vol. 52, pp. 606–613, 2015.

[20] M. R. Schurgot, D. A. Shinberg, and L. G. Greenwald, "Experiments with security and privacy in IoT networks," in *Proceedings of IEEE World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Boston, MA, USA, June 2015.

[21] 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.

[22] T. U. Darmstadt, "Security and privacy challenges in industrial internet of things," in *Proceedings of 52nd Annual Design Automation Conference*, pp. 1–6, San Francisco, CA, USA, June 2015.

[23] S. J. Kumar and D. R. Patel, "A survey on internet of things: security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20–26, 2014.

[24] J. Daubert, W. Alexander, and P. Kikiras, "A view on privacy & trust in IoT," in *Proceedings of IOT/CPS-Security Workshop IEEE International Conference on Communications (ICC)*, London, UK, June 2015.

[25] X. Lu, Q. Li, Z. Qu, and P. Hui, "Privacy information security classification study in internet of things," in *Proceedings of 2014 International Conference on Identification, Information and Knowledge in the Internet of Things*, pp. 162–165, Beijing, China, October 2014.

[26] J.-L. Hou and K.-H. Yeh, "Novel authentication schemes for IoT based healthcare systems," *International Journal of Distributed Sensor Networks*, vol. 11, no. 11, article 183659, 2015.

[27] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, "Key management protocol with implicit certificates for IoT systems," in *Proceedings of Workshop on IoT challenges in Mobile and Industrial Systems-IoT-Sys*, pp. 37–42, Florence, Italy, May 2015.

[28] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Networks*, vol. 32, pp. 17–31, 2015.

[29] F. I. Khan and S. Hameed, "Software defined security service provisioning framework for internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 12, 2016.

[30] O. Garcia-morchon, R. Rietman, and I. E. Shparlinski, "Interpolation and approximation of polynomials in finite fields over a short interval from noisy values," *Experimental Mathematics*, vol. 23, no. 3, pp. 241–260, 2014.

[31] O. Garcia-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, and J. L. Torre-Arce, "DTLS-HIMMO: efficiently securing a post-quantum world with a fully collusion resistant KPS," IACR cryptology, 2014.

[32] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-End transport security in the IP-based internet of things," in *Proceedings of 21st International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–5, Munich, Germany, July–August 2012.

[33] O. Garcia-Morchon, D. Gomez-Perez, J. Gutierrez, R. Rietman, B. Schoenmakers, and L. Tolhuizen, "HIMMO-a lightweight collusion resistant key predistribution scheme," in *Proceedings of IACR 2015*, Mumbai, India, 2015.

[34] O. Garcia-Morchon, R. Rietman, L. Tolhuizen, D. Gomez, and J. Gutierrez, "The MMO problem," in *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, New York, NY, USA, July 2014.

[35] O. Garcia-Morchon, L. Tolhuizen, D. Gomez, and J. Gutierrez, "Towards fully collusion-resistant ID-based establishment of pairwise keys," in *Proceedings of Extended Abstracts of the Third Workshop on Mathematical Cryptology (WMC 2012) and the Third International Conference on Symbolic Computation and Cryptography (SCC 2012)*, pp. 30–36, Castro Urdiales, Spain, July 2012.

[36] O. Morchon, H. Baldus, and D. Sanchez, "Resource-efficient security for medical body sensor networks," in *Proceedings of Wearable and Implantable Body Sensor Networks, BSN 2006*, pp. 80–83, Cambridge, MA, USA, April 2006.

[37] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[38] J. L. Hernandez-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a lightweight authentication and authorization framework for smart objects," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 4, pp. 690–702, 2015.

[39] G. Peretti, V. Lakkundi, and M. Zorzi, "BlinkToSCoAP: an end-to-end security framework for the internet of things," in *Proceedings of Communication Systems and Networks (COMSNETS)*, pp. 1–6, Bangalore, India, January 2015.

[40] D. Dinu, A. Biryukov, and J. Großsch, "FELICS fair evaluation of lightweight cryptographic systems," in *Proceedings of NIST Workshop on Lightweight Cryptography*, Gaithersburg, MD, USA, April 2015.

[41] L. Seitz, G. Selander, and C. Gehrmann, "Authorization framework for the internet-of-things," in *Proceedings of World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–6, Sydney, Australia, June 2013.

[42] G. Piro, G. Boggia, and L. a. Grieco, "A standard compliant security framework for IEEE 802.15.4 networks," in *Proceedings of Internet of Things (WF-IoT)*, pp. 27–30, Seoul, South Korea, March 2014.

[43] X. Huang, P. Craig, H. Lin, and Z Yan, "SecIoT: a security framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 16, pp. 3083–3094, 2015.

[44] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," in *Proceedings of Local Computer Networks, LCN (2012)*, pp. 956–963, Clearwater Beach, FL, USA, October 2012.

[45] J. Granjal, E. Monteiro, and J. S. Silva, "On the effectiveness of end-to-end security for internet-integrated sensing applications," in *Proceedings of 2012 IEEE International Conference on Green Computing and Communications*, pp. 87–93, Besancon, France, November 2012.

[46] S. Hameed, B. Hameed, S. A. Hussain, and W. Khalid, "Lightweight security middleware to detect malicious content in NFC tags or smart posters," in *Proceedings of 2014 IEEE 13th International Conference on Trust, Security and Privacy in*

Computing and Communications (TrustCom), pp. 900–905, Beijing, China, September 2014.

[47] S. Hameed, U. M. Jamali, and A. Samad, "Integrity protection of NDEF message with flexible and enhanced NFC signature records," in *2015 IEEE Proceedings of Trustcom/BigDataSE/ISPA*, vol. 1, pp. 368–375, Helsinki, Finland, August 2015.

[48] S. Hameed, U. M. Jamali, and A. Samad, "Protecting NFC data exchange against eavesdropping with encryption record type definition," in *Proceedings of 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS)*, pp. 577–583, Taipei, Taiwan, April 2016.

[49] S. Md Zin, N. Badrul Anuar, M. L. M. Kiah, and A.-S. K. Pathan, "Routing protocol design for secure WSN: review and open research issues," *Journal of Network and Computer Applications*, vol. 41, pp. 517–530, 2014.

[50] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad-hoc routing for wireless networks," in *Proceedings of 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, Long Beach, CA, USA, 2001.

[51] T. Heer, S. G¨otz, O. Morchon, and K. Wehrle, "Alpha: an adaptive and lightweight protocol for hop-by-hop authentication," in *Proceedings of ACM CoNEXT Conference*, Madrid, Spain, December 2008.

[52] D. Tang, T. Li, J. Ren, and J. Wu, "Cost-aware SEcure routing (CASER) protocol design for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 960–973, 2014.

[53] N. Lasla, A. Derhab, A. Ouadjaout, M. Bagaa, and Y. Challal, "SMART: secure multi-paths routing for wireless sensor networks," in *Proceedings of International Conference on Ad-Hoc Networks and Wireless*, Benidorm, Spain, June 2014.

[54] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," in *Proceedings of IEEE World Forum of Internet of Things (WF-IoT)*, Reston, VA, USA, December 2014.

[55] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: a trust aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 1, pp. 1–14, 2014.

[56] R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, and M. Rossi, "Secure communication for smart IoT objects: protocol stacks, use cases and practical examples," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–7, San Francisco, CA, USA, June 2012.

[57] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, article 794326, 2013.

[58] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proceedings of 2013 Ninth International Conference on Computational Intelligence and Security*, pp. 663–667, Sichan Province, China, December 2013.

[59] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of ACM Workshop on Wireless Security*, pp. 1–10, Atlanta, GA, USA, September 2002.

[60] D. Cerri and A. Ghioni, "Securing AODV: the A-SAODV secure routing prototype," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 120–125, 2008.

[61] Y. W. Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[62] J. Cordasco and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 2, pp. 131–140, 2008.

[63] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, 2006.

[64] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for internet of things," in *Proceedings of 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 606–611, Ottawa, ON, Canada, May 2015.

[65] N. B. Priyantha, A. Kansal, M. Goraczko, and F. Zhao, "Tiny web services : design and implementation of interoperable and evolvable sensor networks," in *Proceedings of 6th ACM Conference on Embedded Network Sensor Systems*, pp. 253–266, Raleigh, NC, USA, November 2008.

[66] S. Br, S. Weißleder, and M. Malek, "A fault taxonomy for service-oriented architecture," in *Proceedings of High Assurance Systems Engineering Symposium*, pp. 367-368, Dallas, Texas, USA, November 2007.

[67] X. Wang, J. Wang, Z. Zheng, Y. Xu, and M. Yang, "Service composition in service-oriented wireless sensor networks with persistent queries," in *Proceedings of 6th IEEE Consumer Communications and Networking Conference*, pp. 1–5, Las Vegas, NV, USA, June 2009.

[68] D. Kuptsov, A. Gurtov, O. G. Morchon, and K. Wehrle, "Brief announcement: distributed trust management and revocation," in *Proceedings of 29th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing*, pp. 233-234, Zurich, Switzerland, July 2010.

[69] O. Garcia-Morchon, D. Kuptsov, A. Gurtov, and K. Wehrle, "Cooperative security in distributed networks," *Computer Communications*, vol. 36, no. 12, pp. 1284–1297, 2013.

[70] O. Garcia-Morchon and K. Wehrle, "Efficient and context-aware access control for pervasive medical sensor networks," in *Proceedings of 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp. 322–327, Mannheim, Germany, 2010.

[71] V. Singhvi, A. Krause, C. Guestrin, J. Garrett, and H. S. Matthews, "Intelligent light control using sensor networks," in *Proceedings of SenSys 2005*, San Diego, CA, USA, November 2005.

[72] R. Kamal, C. S. Hong, and S. Member, "Autonomic resilient internet-of things (IoT) management," 2015, http://arxiv.org/abs/1508.03975.

[73] S. Misra, A. Gupta, P. V. Krishna, H. Agarwal, and M. S. Obaidat, "An adaptive learning approach for fault-tolerant routing in internet of things," in *Proceedings of 2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 815–819, Paris, France, April 2012.

[74] X. Li, H. Ji, and Y. Li, "Layered fault management scheme for end-to-end transmission in internet of things," *Mobile Networks and Applications*, vol. 18, no. 2, pp. 195–205, 2012.

[75] P. H. Su, C. S. Shih, J. Y. J. Hsu, K. J. Lin, and Y. C. Wang, "Decentralized fault tolerance mechanism for intelligent IoT/M2M middleware," in *Proceedings of IEEE World Forum on Internet of Things WF-IoT 2014*, Seoul, Republic of Korea, March 2014.

[76] Y. Liu, Y. Yang, X. Lv, and L. Wang, "A self-learning sensor fault detection framework for industry monitoring IoT,"

Mathematical Problems in Engineering, vol. 2013, Article ID 712028, 8 pages, 2013.

[77] M. Rajan, P. Balamuralidhar, K. Chethan, and M. Swarnahpriyaah, "A self-reconfigurable sensor network management system for internet of things paradigm," in *Proceedings of 2011 International Conference on Devices and Communications (ICDeCom)*, Ranchi, India, February 2011.

[78] K. An, "Resource management and fault tolerance principles for supporting distributed real-time and embedded systems in the cloud," in *Proceedings of Doctoral Symposium on International Middleware Conference*, pp. 1–6, Montreal, Canada, December 2012.

[79] M. Fazio, A. Celesti, A. Puliafito, and M. Villari, "An integrated system for advanced multi-risk management based on cloud for IoT," in *Advances in Intelligent Systems and Computing*, pp. 253–269, Springer, Berlin, Germany, 2014.

[80] J. Kim, S. Yu, and J. Lee, "Wireless sensor network management for sustainable internet of things," in *Proceedings of 2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 177-178, Seoul, Republic of Korea, March 2014.

[81] T. N. Gia, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fault tolerant and scalable IoT-based architecture for health monitoring," in *Proceedings of IEEE Sensors Applications Symposium*, pp. 1–6, Catania, Italy, April 2015.

[82] C. Sommer, F. Hagenauer, and F. Dressler, "A networking perspective on self-organizing intersection management," in *Proceedings of Internet of Things (WFIoT)*, pp. 230–234, Seoul, Republic of Korea, March 2014.

[83] V. Cackovic and Z. Popovic, "Management in M2M networks," in *Proceedings of 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 501–506, Opatija, Croatia, May 2014.

[84] C. P. Mayer, "Security and privacy challenges in the internet of things," *Electronic Communication of the European Association of Software Science and Technology-ECEASST*, vol. 17, pp. 1–12, 2009.

[85] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems*, vol. 24, no. 2, pp. 115–139, 2006.

[86] Y. Hu, Y. Wu, and H. Wang, "Detection of insider selective forwarding attack based on monitor node and trust mechanism in WSN," *Wireless Sensor Network*, vol. 6, no. 11, pp. 237–248, 2014.

[87] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in *Proceedings of INFOCOM*, pp. 1937–1945, Anchorage, AK, USA, 2007.

[88] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Detecting sybil attacks in wireless sensor networks using UWB ranging-based information," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7560–7572, 2015.

[89] D. Juneja and N. Arora, "An ant based framework for preventing DDoS Attack in wireless sensor networks," *International Journal of Advancements in Technology*, vol. 1, no. 1, pp. 34–44, 2010.

[90] V. Nigam, S. Jain, and K. Burse, "Profile based scheme against DDoS attack in WSN," in *Proceedings of Communication Systems and Network Technologies (CSNT)*, pp. 112–116, Bhopal, India, April 2014.

[91] A. D. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press, Boca Raton, FL, USA, 2004.

[92] D. Yang, A. Usynin, and J. Hines, "Anomaly-based intrusion detection for SCADA systems," in *Proceedings of 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC&HMIT 05)*, pp. 12–16, 2005.

[93] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of service detection in 6LoWPAN based internet of things," in *Proceedings of International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 600–607, Lyon, France, 2013.

[94] N. Ruan and Y. Hori, "DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things," in *Proceedings of International Conference on Selected Topics in Mobile and Wireless Networking*, Avignon, France, 2012.

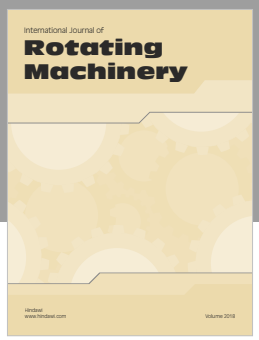
[95] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata based solution for preventing distributed denial of service in internet of things," in *Proceedings of International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, pp. 114–122, Dalian, China, 2011.

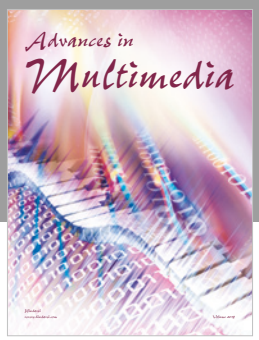
[96] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, and M. A. Spirito, "DEMO: an IDS framework for internet of things empowered by 6LoWPAN," in *Proceedings of ACM SIGSAC Conference on Computer & Communications Security*, Berlin, Germany, November 2013.

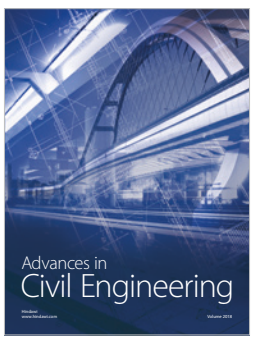
[97] P. Pongle and G. Chavan, "A survey: attacks on RPL and 6LoWPAN in IoT," in *Proceedings of International Conference on Pervasive Computing (ICPC)*, 2015.

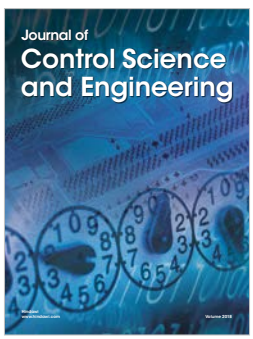
[98] S. Hameed and U. Ali, "HADEC: hadoop-based live DDoS detection framework," *EURASIP Journal on Information Security*, vol. 2018, no. 1, p. 11, 2018.

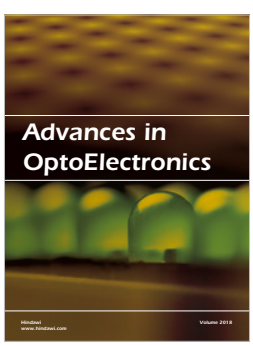
[99] S. Hameed and H. A. Khan, "SDN based collaborative scheme for mitigation of DDoS attacks," *Future Internet*, vol. 10, no. 3, p. 23, 2018.

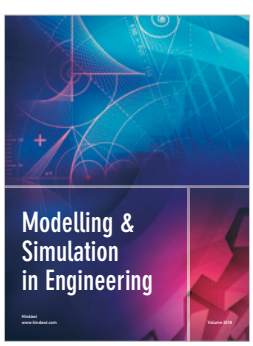


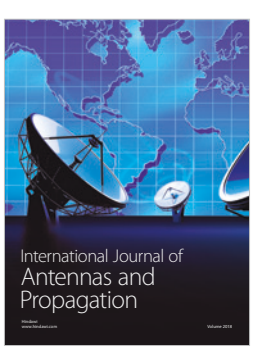


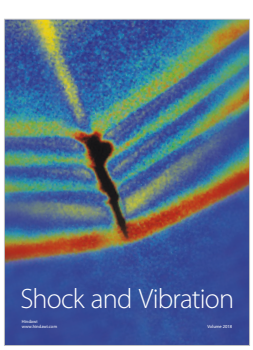


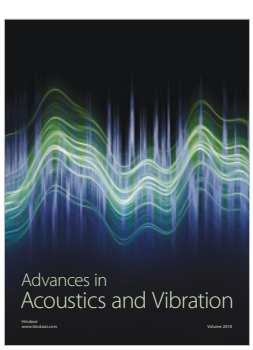












Hindawi

Submit your manuscripts at
www.hindawi.com