Hindawi Publishing Corporation
Journal of Sensors
Volume 2015, Article ID 827546, 10 pages
http://dx.doi.org/10.1155/2015/827546

Research Article

Mobile Device Based Dynamic Key Management Protocols for Wireless Sensor Networks

Chin-Ling Chen,[1] Chih-Cheng Chen,[2] and De-Kui Li[3]

[1]*Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan*
[2]*Department of Health Policy and Management, Chung Shan Medical University, Taichung 40201, Taiwan*
[3]*Department of Information Management, Liaocheng University, Liaocheng, Shandong 252000, China*

Correspondence should be addressed to De-Kui Li; jerryinkorea@gmail.com

Received 25 March 2015; Revised 28 June 2015; Accepted 6 July 2015

Academic Editor: James J. Park

In recent years, wireless sensor network (WSN) applications have tended to transmit data hop by hop, from sensor nodes through cluster nodes to the base station. As a result, users must collect data from the base station. This study considers two different applications: hop by hop transmission of data from cluster nodes to the base station and the direct access to cluster nodes data by mobile users via mobile devices. Due to the hardware limitations of WSNs, some low-cost operations such as symmetric cryptographic algorithms and hash functions are used to implement a dynamic key management. The session key can be updated to prevent threats of attack from each communication. With these methods, the data gathered in wireless sensor networks can be more securely communicated. Moreover, the proposed scheme is analyzed and compared with related schemes. In addition, an NS2 simulation is developed in which the experimental results show that the designed communication protocol is workable.

1. Introduction

In recent years, wireless sensor networks (WSNs) have been used to extensively monitor physical environments, emerging as an important component in the fusion of wireless networks. These tiny sensors make use of wireless communication to process data and require security protocols for safety during communication. The sensor, however, has limited scope as a result of its power supply and the distance of the wireless communication. Due to this limited power and delivery distance, multihop methods are used to transmit data. Thus, the sensor can monitor the environment and process the data collected from the networks, transmitting it to cluster nodes or a base station. Due to the use of wireless communication, latent attacks on data frequently occur during transmission.

WSNs [1, 2] have certain characteristics that make them adaptable to various areas, including their small size and low costs. The advantage of these sensors is that their small size with smaller memory size makes them portable but limits their capabilities in high cost operations. Due to these properties, this study proposes a combination of low-cost operation and user authentication to enhance security in WSN communication.

A key management procedure is an essential constituent of network security. Symmetric key systems require the keys to be kept out of reach of potential attackers. Because of the resource constraints and the lack of the infrastructure support, key distribution and management are much more difficult in WSNs than in their traditional wired and wireless counterparts [3].

Public key-based asymmetric cryptographic algorithms [4] are not suitable for sensor networks. This is why new security protocols or mechanisms need to be proposed to meet the new emerging security requirements for WSNs. The symmetric key approach is an appropriate cryptography for wireless sensors due to its low energy consumption and simple hardware requirements, but the distribution of symmetric keys into sensor nodes presents a significant challenge [5]. Many researchers [6–11] have focused on this area recently and proposed several key management schemes to establish the session key between sensor nodes. However, these schemes [6–11] do not support mobile users directly accessing cluster node data via mobile device. For example,

the administrators of farms or nuclear power plants can use mobile devices to gain access to the monitor data at any time from any place, rather than logging into the monitor system. Moreover, as sensor networks have energy and computational constraints, it is therefore necessary to maintain a balanced security level with respect to those constraints.

Since sensor networks can be used in a variety of applications, such as military sensing and tracking, environmental monitoring, patient monitoring and tracking, smart environments, and disaster management, this study envisages many applications in which people could navigate through sensor networks using common omnipresent devices (such as a mobile phone or a personal digital assistant) at any time and from anywhere. Since a mobile device is more portable and personal than a personal computer, it is more convenient for operating certain applications.

Some applications [12–14] have proposed novel solutions to remote user authentication by using smart cards. The smart card is a processor that can compute some low-cost operations, such as one-way hash function and exclusion-OR operation. In the proposed system, each user is issued with a smart card for login and authentication. These lightweight operations are similar to the processors of sensor nodes in WSNs. In addition, there have been authentication schemes based on the ElGamal cryptosystem [15, 16] that belong to a public key cryptosystem. Owing to their high operation costs, these schemes are not suitable for WSNs.

Password-based authentication is the most widely used method for remote user authentication. Existing schemes can be categorized into two types: the weak password approach and the strong password approach. The weak password approach is based on the ElGamal cryptosystem. Its advantage lies in the fact that it does not need a user ID-password table to verify the validity of the user login. Unfortunately, the weak password approach places a heavy computational load on the system, and remote sensor nodes lack the capacity for rendering the system applicable to WSNs. The strong password approach is based on one-way hash function and exclusive-OR (XOR) operations. The one-way hash function $h(\ )$ has the following properties: (1) $h(x)$ is relatively easy to compute for any given x, making both hardware and software implementation practical. (2) For any given value y, it is computationally infeasible to find x such that $h(x) = y$. (3) For any given block x, it is computationally infeasible to find $y \neq x$ with $h(y) = h(x)$. This is sometimes referred to as weak collision resistance. Das et al. [17] proposed a dynamic ID-based remote user authentication scheme in 2004. It requires much less computation and needs only simple operations. For this reason, this scheme has certain advantages when applied to a WSN environment.

In 2002, El-Fishway and Tadros [18] proposed a user authentication scheme oriented for mobile users using the Global System for Mobile Communication (GSM). The advantage of using GSM is that there is no central certification authority, but the scheme requires high computation costs by the public key system. Thus, a user authentication scheme of the public key system is unsuitable for WSNs. In 2010, Chen [19] proposed a mobile DRM mechanism based on PKI (Public Key Infrastructure). He also emphasizes that the mobile device should be operated in a lightweight environment.

In this paper, we use some lightweight operations (such as symmetric encryption/decryption, hash function) to implement a dynamic key management scheme. The proposed scheme also supports a direct accessing of cluster node data by a user via mobile device at anytime from anywhere and provides more security analysis; refer to related works. The organization of the remainder of the paper is as follows. In Section 2, the proposed protocol is presented. In Section 3, several familiar attacks and the performance of the proposed scheme are analyzed. Comparison is also made with other related schemes in Section 4. Finally, Section 5 offers conclusions.

2. The Proposed Scheme

2.1. Notations. The following is the introduction to the notations that will be used in our scheme.

$h(\ )$ is a one-way hash function.

Cert_k is the kth mobile user's digital certificate.

$\text{ID}_{\text{mob}k}$ is the identity of the kth mobile user.

ID_{ci} is the identity of the ith cluster node.

ID_B is the identity of the base station.

RND is a random number generated by mobile user.

PW is the mobile user's password.

$K_{ci}^{(j)}$ is the jth updated session keys of the ith cluster node, where $K_{ci}^{(j)} = h(K_{ci}^{(j-1)}, K_{ci}^{(j-2)})$, with $K_{ci}^{(0)} = a$; $K_{ci}^{(1)} = b$, and a and b are the initial random numbers.

M_{req} is request message issued by mobile user.

M_c is the latest information received from the cluster node.

$M_{\text{upd-key}}$ is the message of the updated key.

$E(\text{msg}, K)$ is the symmetric encryption of the infrastructure that makes use of key K to encrypt msg.

$D(C, K)$ is the symmetric decryption of the infrastructure that makes use of key K to decrypt the ciphertext C.

$X \stackrel{?}{=} Y$ compares whether X is equal to Y or not.

2.2. Environmental Conditions

(1) As a general rule, hundreds or even thousands of sensor nodes are deployed in a WSN. In this paper, cluster management is used to transmit data. Additionally, the deployed sensor nodes are divided into different regions so that each sensor node can transmit data in the effective range [9].

(2) In each of the regions, a sensor node is chosen automatically as a cluster node [20–22]. These related algorithms are similar to those used by Park and

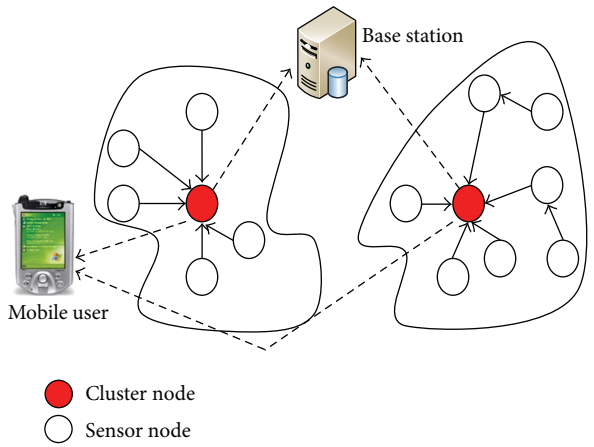


Figure 1: Transmission paths of the sensor network.

Corson [23], Perkins and Royer [24], and Johnson and Maltz [25]. Once the cluster node has received a certain number of packets, the data is transmitted to the base station. The user can also use a mobile device to access data from the cluster node. To achieve better performance and security, a heterogeneous sensor network model consisting of a small number of powerful high-end sensors (H-sensors) (e.g., PDAs or cellular phones) and a large number of low-end sensors (L-sensors) (e.g., the small MICA2 sensors, manufactured by Crossbow Technology) are adopted [26]. L-sensors are ordinary sensor nodes with limited computation, communication, energy supply, and storage capability. The transmission paths of the sensor network are shown in Figure 1. Additionally, in a heterogeneous sensor network (HSN) [27, 28], more types of different nodes with different levels of battery energy and functionality are employed. It may be argued that, by using a few designated nodes with complex hardware, extra battery energy, and additional functionalities, while keeping the rest of the nodes simple, the total cost of hardware in the network can be minimized to offer a longer life span.

(3) Once each of the cluster nodes is dispatched from the factory, it is preset according to the parameters b_i and b_{i-1}. A new key is generated by a one-way hash function (e.g., $K_{ci} = h(b_i, b_{i-1})$) to communicate with the base station.

(4) When the cluster node has received a certain number of packets, the data is arranged, encrypted, and transmitted to the backend base station. When the base station receives the packet from the cluster node, it will update the cluster node's key, successfully decrypting the ciphertext to the next communication.

(5) Since the size of the sensor node is limited, its memory capacity is also limited. The memory capacity of each sensor node is 512 K bytes. When the security of the WSN is enhanced, the memory capacity of sensor nodes should also be taken into account.

(6) The CPU is fixed in the sensor node to handle and calculate the data. This limited size and power supply only allowed for a low-end CPU model such as the StrongARM [29] from Intel and ATmega [30] from Atmel, which are commonly used.

2.3. Registration Phase. In order to allow mobile users to directly communicate with cluster nodes at anytime from anywhere, in the registration phase, mobile users register with a base station, which will send a certificate to the mobile users. After registering, the mobile users can communicate directly with the cluster node.

The cluster node will receive the authenticated data from the base station if a mobile user chooses to receive data. Since the cluster nodes are predeployed in advance, it is assumed that the communication channel is insecure between the cluster node and the base station in the registration phase. Unlike the communication between the cluster node and the base station, the communication channel is secure between the mobile user and the base station in the registration phase. The proposed registration phase is divided into the following steps. The scenarios are shown in Figure 2.

(1) Mobile user $\rightarrow$ base station: $(M_{\text{req}}, \text{ID}_{\text{mob}k}, \text{PW}, \text{RND})$.

When a mobile user wants to communicate with the cluster node, it must obtain a digital certificate Cert_k from the base station in advance. The mobile user makes a request message M_{req} and chooses a password PW and random number RND. The mobile user transmits $(M_{\text{req}}, \text{ID}_{\text{mob}k}, \text{PW}, \text{RND})$ to the base station via the secure channel.

(2) Base station $\rightarrow$ mobile user: $(\text{Cert}_k, \text{ID}_{ci}, K_{ci}^{(j)})$.

Base station $\rightarrow$ cluster node: C_{clu}.

Once the base station receives the above request message from the mobile user, the base station issues a certification Cert_j, to determine the correct cluster node ID_{ci}, allowing the mobile user to communicate and compute

$$A = h\left(\text{ID}_{\text{mob}k} \| \text{PW} \| \text{RND}\right). \quad (1)$$

The base station stores $(\text{ID}_{\text{mob}k}, \text{ID}_{ci}, K_{ci}^{(j)}, A)$ in its database. The messages $(\text{Cert}_k, \text{ID}_{ci}, K_{ci}^{(j)})$ are transmitted to the mobile user. At that moment, the base station uses $K_{ci}^{(j)}$ to encrypt RND as a complete packet C_{clu} in the following manner:

$$C_{\text{clu}} = E\left(\left(\text{ID}_{\text{mob}j}, \text{RND}\right), K_{ci}^{(j)}\right). \quad (2)$$

Then, the C_{clu} is transmitted to the cluster node.

(3) Upon receiving the packet C_{clu}, the cluster node uses the session key $K_{ci}^{(j)}$ to decrypt C_{clu} and obtain $\text{ID}_{\text{mob}j}$ and the random number RND:

$$\left(\text{ID}_{\text{mob}j}, \text{RND}\right) = D\left(C_{\text{clu}}, K_{ci}^{(j)}\right). \quad (3)$$

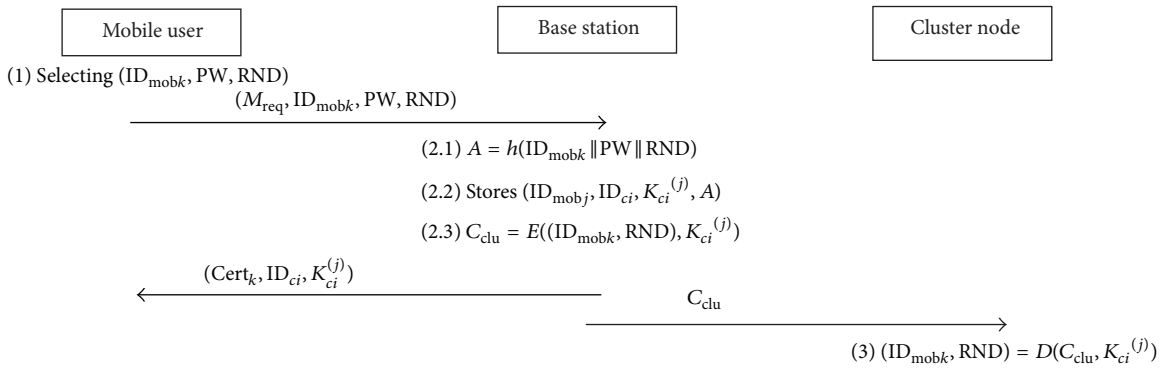


Figure 2: The registration phase protocol.

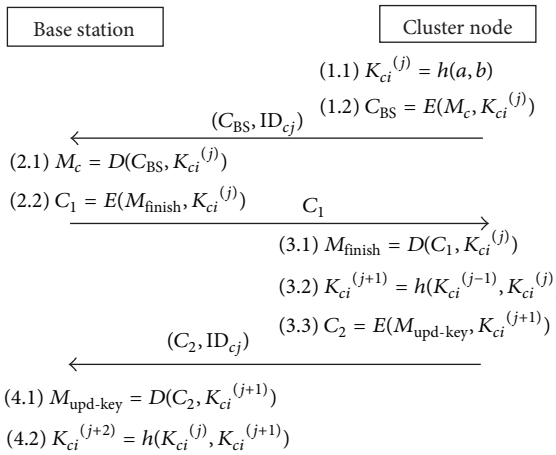


Figure 3: The communication phase protocol between the base station and the cluster node.

2.4. The Communication Phase Protocol between Base Station and Cluster Node. This study proposes a dynamic key management mechanism with two keys preset in each sensor node, cluster node, and a new key for the next round generated by the previous two keys.

The new session key is updated after each round between the base station and the cluster node. The cluster nodes periodically respond to the collected data sent to the base station. The proposed protocol is divided into the following four steps, as shown in Figure 3.

(1) Cluster node → base station: (C_{BS}, ID$_{cj}$).

The cluster node uses the preset parameters a and b to generate a session key

$$K_{ci}^{(j)} = h(a, b). \tag{4}$$

When the deployed cluster node returns the collected information M_c, the cluster node will transmit the information to the base station periodically. The cluster node uses $K_{ci}^{(j)}$ to encrypt M_c as a complete packet C_{BS}:

$$C_{BS} = E\left(M_c, K_{ci}^{(j)}\right). \tag{5}$$

Together with the code ID$_{ci}$ of the cluster node, (C_{BS}, ID$_{cj}$) is transmitted to the base station.

(2) Base station → cluster node: C_1.

When the base station receives the packet from the cluster node, it confirms the code ID$_{cj}$ of the cluster node and seeks the session key $K_{ci}^{(j)}$ of that cluster node in the database. $K_{ci}^{(j)}$ is used to decrypt M_C as follows:

$$M_C = D\left(C_{BS}, K_{ci}^{(j)}\right). \tag{6}$$

Therefore, the base station can receive the collected data M_C from the cluster node. It can then access this information and send the finished message M_{finish} to the cluster node. At that moment, the base station uses $K_{ci}^{(j)}$ to encrypt M_{finish}. The encrypted data C_1 will be returned to the cluster node:

$$C_1 = E\left(M_{finish}, K_{ci}^{(j)}\right). \tag{7}$$

(3) Cluster node → base station: (C_2, ID$_{ci}$).

When the cluster node receives the returned data from the base station, it uses the session key $K_{ci}^{(j)}$ to decrypt C_1 as follows:

$$M_{finish} = D\left(C_1, K_{ci}^{(j)}\right). \tag{8}$$

The cluster node updates the session key, and ($K_{ci}^{(j-1)}$ and $K_{ci}^{(j)}$) are used to generate a new session key $K_{ci}^{(j+1)}$

$$K_{ci}^{(j+1)} = h\left(K_{ci}^{(j-1)}, K_{ci}^{(j)}\right). \tag{9}$$

At that moment, the cluster node uses $K_{ci}^{(j+1)}$ to encrypt the updated key message $M_{upd\text{-}key}$ as a complete packet

$$C_2 = E\left(M_{upd\text{-}key}, K_{ci}^{(j+1)}\right) \tag{10}$$

and sends (C_2, ID$_{ci}$) to the base station.

(4) The base station receives the packet from the cluster node and uses $K_{ci}^{(j+1)}$ to decrypt and obtain the message $M_{upd\text{-}key}$ as follows:

$$M_{upd\text{-}key} = D\left(C_2, K_{ci}^{(j+1)}\right). \tag{11}$$

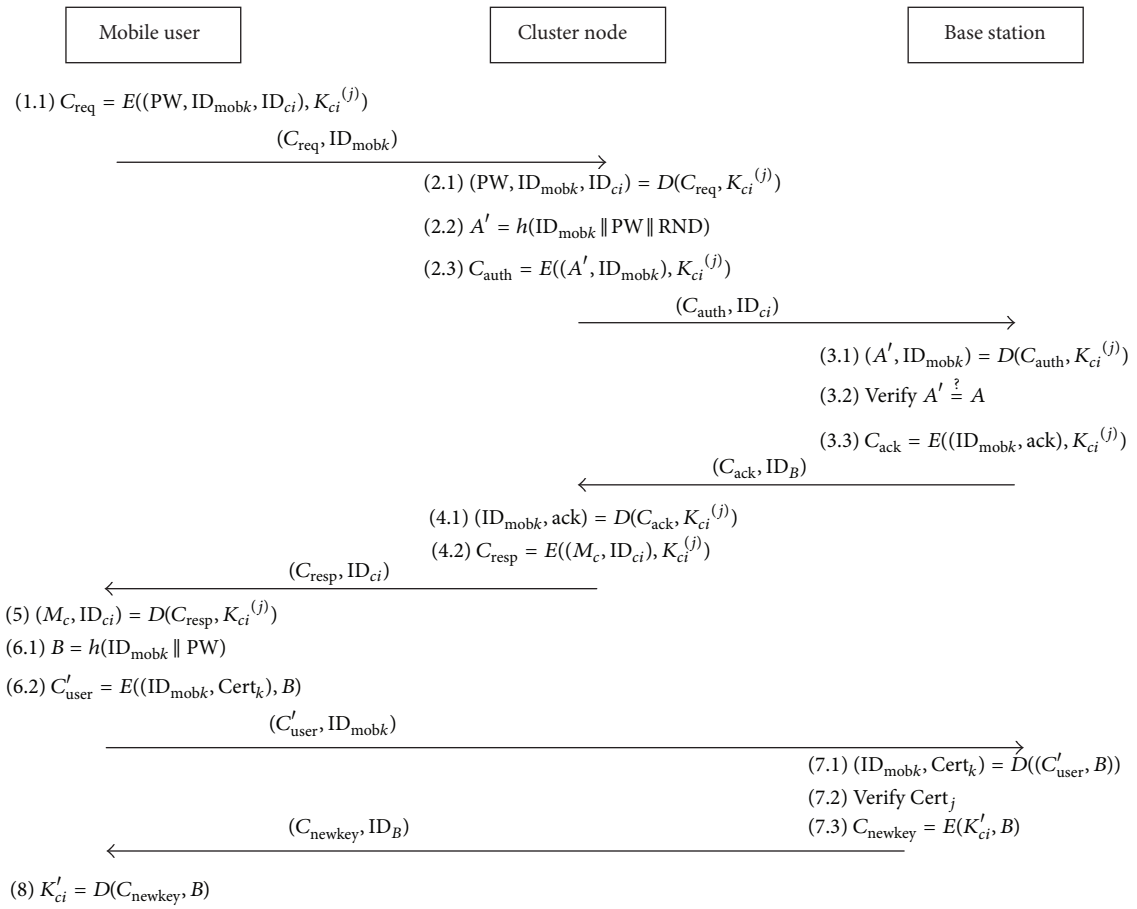


Figure 4: The communication phase protocol between the mobile user, the cluster node, and the base station.

For the same reason, the base station will use the $K_{ci}^{(j)}$ and $K_{ci}^{(j+1)}$ to update the new session key $K_{ci}^{(j+2)}$ for the next transaction:

$$K_{ci}^{(j+2)} = h\left(K_{ci}^{(j)}, K_{ci}^{(j+1)}\right). \tag{12}$$

2.5. Communication Phase Protocol between Mobile User, Cluster Node, and Base Station. The mobile user can also obtain the data from the cluster node through the communication phase. When the cluster node receives the request, it authenticates the identity of the mobile user. If the mobile user is authenticated as legal, the cluster node will transmit the collected data to the mobile user. When the mobile user receives the data from a cluster node, it can use the session key of the cluster node to decrypt it. If the key is overdue, the user should communicate with the base station to update the session key and decrypt the received data. These scenarios are shown in Figure 4.

(1) Mobile user $\rightarrow$ cluster node: $(C_{\text{req}}, \text{ID}_{\text{mob}j})$.

When the mobile user wants to obtain data from the cluster node, it uses the last transaction session key with the cluster node, $K_{ci}^{(j)}$, to encrypt password PW, $\text{ID}_{\text{mob}k}$, and ID_{ci}:

$$C_{\text{req}} = E\left(\left(\text{PW}, \text{ID}_{\text{mob}k}, \text{ID}_{ci}\right), K_{ci}^{(j)}\right). \tag{13}$$

The mobile user transmits $(C_{\text{req}}, \text{ID}_{\text{mob}k})$ to the cluster node.

(2) Cluster node $\rightarrow$ base station: $(C_{\text{auth}}, \text{ID}_{ci})$.

The cluster node receives the packet from the kth mobile user and uses the last transaction session key with the mobile user, $K_{ci}^{(j)}$, to decrypt and obtain the complete message:

$$\left(\text{PW}, \text{ID}_{\text{mob}k}, \text{ID}_{ci}\right) = D\left(C_{\text{req}}, K_{ci}^{(j)}\right). \tag{14}$$

The cluster node computes A' as follows:

$$A' = h\left(\text{ID}_{\text{mob}k} \| \text{PW} \| \text{RND}\right). \tag{15}$$

It then uses the key $K_{ci}^{(j)}$ to encrypt A' as follows:

$$C_{\text{auth}} = E\left(\left(A', \text{ID}_{\text{mob}k}\right), K_{ci}^{(j)}\right). \tag{16}$$

It then transmits the packet $(C_{\text{auth}}, \text{ID}_{ci})$ to the base station.

(3) Base station $\rightarrow$ cluster node: $(C_{\text{ack}}, \text{ID}_B)$.

The base station receives the packet $(C_{\text{auth}}, \text{ID}_{ci})$ from the cluster node, which uses the key $K_{ci}^{(j)}$ to decrypt the packet C_{auth} as follows:

$$\left(A', \text{ID}_{\text{mob}k}\right) = D\left(C_{\text{auth}}, K_{ci}^{(j)}\right). \tag{17}$$

The base station verifies whether or not $\mathrm{ID}_{\mathrm{mob}k}$ exists in the database. If it can be found, the base station will verify

$$A \stackrel{?}{=} A'. \tag{18}$$

If the equality is not held, the base station abandons the packet; otherwise, the base station uses ${K_{ci}}^{(j)}$ to encrypt the acknowledgement message ack as a packet C_{ack}:

$$C_{\mathrm{ack}} = E\left(\left(\mathrm{ID}_{\mathrm{mob}j}, \mathrm{ack}\right), {K_{ci}}^{(j)}\right) \tag{19}$$

and $(C_{\mathrm{ack}}, \mathrm{ID}_B)$ is then transmitted to the cluster node.

(4) Cluster node $\rightarrow$ mobile user: $(C_{\mathrm{resp}}, \mathrm{ID}_{ci})$.

When the cluster node receives the packet $(C_{\mathrm{ack}}, \mathrm{ID}_B)$, it uses the session key ${K_{ci}}^{(j)}$ to decrypt the acknowledgement message ack to confirm whether or not the mobile user has registered with the base station:

$$\left(\mathrm{ID}_{\mathrm{mob}j}, \mathrm{ack}\right) = D\left(C_{\mathrm{ack}}, {K_{ci}}^{(j)}\right). \tag{20}$$

The cluster node then makes use of ${K_{ci}}^{(j)}$ to encrypt the collected information M_C received from the sensor node and the identification code ID_{ci} as follows:

$$C_{\mathrm{resp}} = E\left(\left(M_C, \mathrm{ID}_{ci}\right), {K_{ci}}^{(j)}\right). \tag{21}$$

Together with ID_{ci}, $(C_{\mathrm{resp}}, \mathrm{ID}_{ci})$ is transmitted and sent to the mobile user as a complete packet.

(5) After the base station receives the packet $(C_{\mathrm{resp}}, \mathrm{ID}_{ci})$, it uses the session key K_{ci} to decrypt and obtain the message M_C:

$$\left(M_C, \mathrm{ID}_{ci}\right) = D\left(C_{\mathrm{resp}}, {K_{ci}}^{(j)}\right). \tag{22}$$

(6) Mobile user $\rightarrow$ base station: $(C'_{\mathrm{user}}, \mathrm{ID}_{\mathrm{mob}k})$.

Since the base station and the cluster node communicate periodically, the cluster node's session key ${K_{ci}}^{(j)}$ is updated for each transaction. Thus, the mobile user's key is likely to be overdue, and the key cannot decrypt C_{resp} smoothly. This means that the key should be updated. The mobile user computes B as follows:

$$B = h\left(\mathrm{ID}_{\mathrm{mob}k} \parallel \mathrm{PW}\right). \tag{23}$$

Later, B is used to encrypt the $\mathrm{ID}_{\mathrm{mob}k}$ and Cert_k as a complete packet C'_{user}, which is generated as follows:

$$C'_{\mathrm{user}} = E\left(\left(\mathrm{ID}_{\mathrm{mob}k}, \mathrm{Cert}_k\right), B\right) \tag{24}$$

and $(C'_{\mathrm{user}}, \mathrm{ID}_{\mathrm{mob}k})$ is then transmitted to the base station.

(7) Base station $\rightarrow$ mobile user: $(C_{\mathrm{newkey}}, \mathrm{ID}_B)$.

After receiving the message C'_{user}, the base station uses B to decrypt and obtain the message $(\mathrm{ID}_{\mathrm{mob}k}, \mathrm{Cert}_k)$ as follows:

$$\left(\mathrm{ID}_{\mathrm{mob}k}, \mathrm{Cert}_k\right) = D\left(C'_{\mathrm{user}}, B\right). \tag{25}$$

The base station uses its public key to verify the digital certificate Cert_k and finds the current cluster node's session key K'_{ci}. The base station uses B to encrypt K'_{ci}:

$$C_{\mathrm{newkey}} = E\left(K'_{ci}, B\right). \tag{26}$$

Along with the codes ID_B, it is transmitted to the mobile user as a complete packet $(C_{\mathrm{newkey}}, \mathrm{ID}_B)$.

(8) Once the mobile user receives the packet from the base station and uses B to decrypt and obtain the K'_{ci},

$$K'_{ci} = D\left(C_{\mathrm{newkey}}, B\right). \tag{27}$$

The mobile user can use the new session key K'_{ci} to decrypt the collected message M_C from the cluster node.

3. Analysis

3.1. Security Analysis

3.1.1. Prevention of Malicious Guessing Attack

Adversary Model 1. Attackers try to intercept sensitive information by guessing the sensitive information.

In the proposed protocol, dynamic key management is used between the cluster node and base station. After a given time, the base station updates the session key with the cluster node. Thus, even if attackers do intercept the sensitive information, they will gain no relevant knowledge about the session key. In this scheme, the base station and cluster nodes update the session key at the end of communication for every round. This communication enhances the security between the base station and the cluster node.

3.1.2. Prevention of Replay Attack

Adversary Model 2. Attackers try to intercept data and retransmit it maliciously or fraudulently repeat or delay it to achieve the purpose of the attack.

In the proposed protocol, the encryption key ${K_{ci}}^{(j)}$ is refreshed for each communication. Therefore, the attackers have no opportunity to achieve the purpose of the attack.

3.1.3. Prevention of the Falsification Attack

Adversary Model 3. Attackers try to impersonate a legal user to achieve a falsification attack.

In the communication phase protocol (Figure 4), the mobile users use the session key ${K_{ci}}^{(j)}$ to encrypt the PW, $\mathrm{ID}_{\mathrm{mob}k}$, and ID_{ci} into a complete packet C_{req}. Once the base station receives the packet, it verifies $A' \stackrel{?}{=} A$. If it is not correct, the cluster node will abandon the packet. The base station can authenticate the mobile user via this authentication mechanism. Therefore, the proposed scheme can prevent the attackers from impersonating a legal user.

Table 1: The time complexity of the proposed communication phase.

Scheme	Role	Time complexity
Communication phase (base station and cluster node, as Figure 3)	Base station	$2T_D + T_E + T_H$
	Cluster node	$T_D + 2T_E + 2T_H$
Communication phase (mobile user, cluster node, and base station, as Figure 4)	Mobile user	$2T_D + 2T_E + T_H$
	Cluster node	$2T_D + 2T_E + T_H$
	Base station	$2T_D + 2T_E + 2T_{\text{COMP}}$

Notes:
T_D: the time complexity of using symmetric decryption algorithm;
T_E: the time complexity of using symmetric encryption algorithm;
T_H: the time taken to execute the hash function;
T_{COMP}: the time for comparing operation.

Table 2: The communication cost of the proposed scheme.

Phase	Rounds	Communication cost	Transmission time (ms)	
			3.6 Mbps	1 Mbps
Registration phase (offline, as Figure 2)	3	$5\lvert M\rvert + \lvert H\rvert + \lvert\text{Cert}\rvert + \lvert C\rvert$	0.092	0.332
Communication phase (base station and cluster node, as Figure 3)	3	$2\lvert M\rvert + 3\lvert C\rvert$	0.038	0.136
Communication phase (mobile user, cluster node, and base station, as Figure 4)	6	$6\lvert M\rvert + 6\lvert C\rvert$	0.093	0.336
Total		$13\lvert M\rvert + \lvert H\rvert + \lvert\text{Cert}\rvert + 10\lvert C\rvert$	0.223	0.804

3.1.4. Prevention of Man-in-the-Middle Attack

Adversary Model 4. Attackers have the ability to both monitor and alter or inject messages into a communication channel.

A cryptography mechanism can be used between the mobile user and the cluster node to encrypt data in order to prevent man-in-the-middle attacks, such as

$$C_{\text{req}} = E\left(\left(\text{PW}, \text{ID}_{\text{mob}k}, \text{ID}_{ci}\right), K_{ci}^{(j)}\right),$$
$$C_{\text{resp}} = E\left(\left(M_C, \text{ID}_{ci}\right), K_{ci}^{(j)}\right). \quad (28)$$

Thus, malicious attackers cannot falsify the protected data. At the end of the communication, the cluster node updates the session key, preventing the attacker from obtaining the node and accessing the protected data. For the same reason, the attacker cannot obtain the protected data M_C, encrypted into C_{BS} (see step 1.2 of Figure 3). Therefore, this scheme can prevent man-in-the-middle attacks.

3.1.5. Dynamic Key Management Attack

Adversary Model 5. Attackers try to guess the key repeatedly. In the proposed infrastructure, for each data transmission, a new key is generated from the previous two keys. For example, if the session keys of the first transaction are $K_{ci}^{(0)} = a$; $K_{ci}^{(1)} = b$, where a and b are the initial random numbers, the jth updated session key of the ith cluster node is $K_{ci}^{(j)} = h(K_{ci}^{(j-1)}, K_{ci}^{(j-2)})$. Because of the secure one-way hash chain, an attacker in possession of the current session key cannot obtain the last session key. This dynamic key management reduces the possibility of attackers correctly guessing the key from the key chain and using it repeatedly.

3.1.6. The Captured Node Attack Analysis

Adversary Model 6. Attackers try to capture nodes and thus obtain sensitive information.

For the mobile user and cluster node transmission or cluster node and base station transmission, the proposed scheme adopts the hash function to generate a one-way key chain $K_{ci}^{(j)}$, $K_{ci}^{(j+1)}$, and $K_{ci}^{(j+2)}$ to encrypt messages, because the one-way hash function can prevent attackers from inverting the key. Therefore, even if an attacker captures a node, he/she cannot gain access to sensitive information. This mechanism is similar to point 5.

3.2. Performance Analysis. This study considers the ramifications of using applications in two different environments: hop by hop transmission of data from cluster nodes to the base station (Figure 3 scenario) and mobile users directly accessing cluster node data via mobile device (Figure 4 scenario). In Table 1, the time complexity in the communication phase is analyzed, and the communication cost of the proposed scheme is analyzed in Table 2.

At the end of this section, the communication values and data transmission times are summarized in Table 2. The length of hash function $|H|$ is 160 bits; it is assumed that the 256-bit pseudorandom number generator is used to generate RND. In order to simplify the length of messages, it is also assumed that the lengths $|M|$ of ID and PW are also 256 bits, the length of digital certificate |Cert| is 1024 bits, and the length of symmetric ciphertext $|C|$ is set to 192 bits.

Table 3: Parameters used in the simulation environment.

Parameter	Values
Simulation tool	NS2
Operating frequency	2.45 GHz
Transmitting power	10 dBm
Receiving sensitivity power	−103 dBm
Battery type	CR2303
Simulation area	1000 m × 1000 m
Number of nodes	300 nodes
Antenna model	Antenna/Omni antenna
Mac type	Mac/802.11.15.4
Interface queue	Query/DropTail/PriQueue
Radio transmission range	30 m~50 m
Data packet size	1456 bits/608 bits/1248 bits
Data transmission rate	3.6 MHz and 1 MHz
Simulation time	28800 seconds (8 hours)
Sensor type	TI CC2530 chip

As shown in Table 2, the two relative transmission rates are 1 Mbps and 3.6 Mbps. Note that, within the environment of 3.6 Mbps, the longest communication cost is required by the communication phase, while the data transmission time is only 0.093 $((6|M| + 6|C|)/(3600 * 8))$ milliseconds.

The total transmission time of the proposed scheme is 0.223 $= ((13|M| + |H| + |\text{Cert}| + 10|C|)/(3600 * 8))$ milliseconds. Since only lightweight operations are used, the transmission time of the proposed scheme is sound.

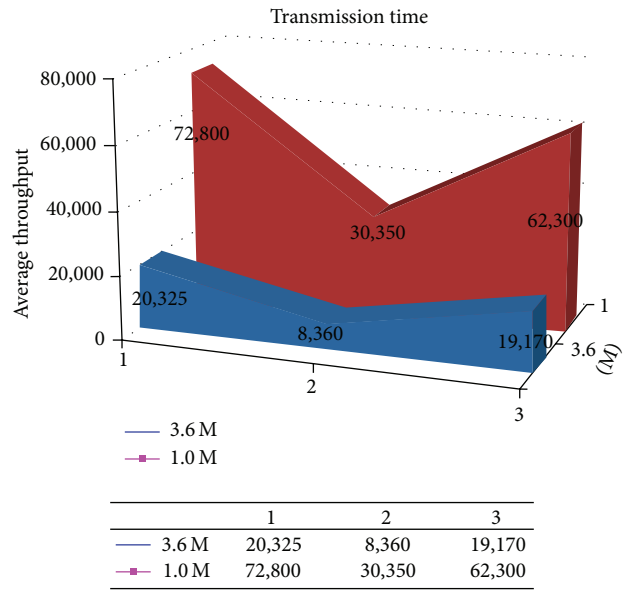
A simulation based on NS2 (Network Simulation 2) is developed, as shown in Table 3.

The IEEE 802.15.4 standard is used in NS2, with an operating frequency of 2.45 GHz, and 10 dBm for transmitting power and receiving sensitivity for −103 dBm. The initial battery type is CR2303. The mobility model is based on the ad hoc model. The sensor nodes are deployed uniformly in a 1000 m × 1000 m field. The simulation lasted for 10 ms. Each simulation was run 50 times (TCP Data Flow). The average throughput of the proposed scheme is shown in Figure 5.

The chip rate of IEEE 802.15.4 in a 2.45 GHz frequency band is 2 MHz, and the chip rate length is 32 when chip period $T_c = 0.5$ ms [31]. If the chip period $T_c = 0.5$ ms, then $F = 1/T = 1/0.5\,\text{ms} = 2000$. Otherwise the chip rate length is 32 and the transmission rate is $2000/32 = 62.5$ Kbps. Because the symbol rate can transmit 4-bit data, the maximum transmission rate is 62.5 Kbps $* 4 = 250$ Kbps. The chip frequency is $2000/32 = 62.5$ Kbps.

Based on the results above, in the registration phase, the average throughput in the 3.6 Mbps frequency band is 20.32 K bps. In the communication phase (base station and cluster node, as in Figure 3), the average throughput is 8.365 Kbps. In the communication phase (mobile user, cluster node, and base station, as in Figure 4), the average throughput is 19.171 Kbps.

In the registration phase, the average throughput in the 1 frequency band is 72.648 Kbps. In the communication phase (base station and cluster node, as in Figure 3), the average throughput is 30.351 Kbps. In the communication phase (mobile user, cluster node, and base station, as in Figure 4), the average throughput is 62.3 Kbps.



	1	2	3
3.6 M	20,325	8,360	19,170
1.0 M	72,800	30,350	62,300

Figure 5: The comparison of the average throughput of the proposed scheme in various different phases. Remark: 1, 2, and 3 denoted in the top row of the table are the transmission time of the registration phase, communication phase protocol between the base station and the cluster node, and communication phase protocol among the mobile user, the cluster node, and the base station, respectively.

According to the IEEE 802.15.4 standard in 2.45 GHz, the maximum transmission rate is 250 Kbps. The communication protocol designed has a rate much lower than 250 Kbps.

In the following section. A comparison of the average throughput of the related works for various different phases in 3.6 Mps and 1 Mps frequency bands is shown in Figure 5.

4. Discussions

In this section, a comparison is made with the related works in Table 4. A complete security analysis has been presented for the proposed scheme. These security issues include malicious guessing attacks, replay attacks, falsification attacks, man-in-the-middle attacks, dynamic key management attacks, and captured node attacks. The security analysis of the proposed scheme is more complete; refer to "Cheng and Agrawal's scheme [6]" and "Liu and Ning's scheme [7]." Compared with the partial analysis of "Cheng and Agrawal's scheme" and "Liu and Ning's scheme," the proposed scheme is more complete. Moreover, the proposed scheme also supports direct accessing of cluster node data by a user via mobile device at any time, from anywhere. Cheng and Agrawal's scheme did not propose a clear application. These works were not specific with regard to time complexity, communication cost, and storage cost. The proposed scheme adopted the symmetric encryption/description algorithm, thus making the time complexity, communication cost, and storage cost of key computation are specific.

Table 4: Comparison of the related works.

Protocol	Our scheme	Cheng and Agrawal [6]	Liu and Ning [7]	Alcaraz et al. [27]
Security analysis	Complete	Partial (only captured node attack analysis)	Partial (only captured node attack analysis)	Yes
Provided mobile service	Yes	N/A	N/A	N/A
Proposed application	Yes	N/A	Yes	Yes
Time complexity analysis	Yes	N/A	N/A	N/A
Communication cost analysis	Yes	N/A	N/A	N/A
Stored cost (cluster node)	Two session keys, itself ID, base station ID, mobile user ID, and RND	One session key and two polynomial functions	Not specific (it is dependent on the proposed three schemes; for example, key predistribution scheme overheads = $c(t+2)\log q$)	N/A
The time cost of key computation (cluster node)	As shown in Table 1	$(n \times t_{\text{poly}} \times l)/m$	Not specific	Not specific

Alcaraz et al. [27] offer a complete analysis of key management schemes (KMS), which provides information on how different protocols fit with the properties. Apart from this, it also offers a comprehensive review on how the application requirements and the properties of various key management schemes influence each other. However, it does not provide accessing of cluster node data via mobile device and give a clear illustration of time complexity analysis, communication cost analysis, and storage cost.

5. Conclusions

This study proposed two schemes for accessing collected data through dynamic key management in heterogeneous and homogenous WSN environments. In addition to allowing the base station to periodically collect data from the cluster node, mobile users can also communicate with the latest cluster nodes with immediacy and mobility.

In this study, we use some lightweight cryptography mechanisms (such as symmetric encryption/decryption, hash function, and random number) to implement a dynamic key management scheme. A performance analysis of time complexity and communication cost was also conducted. Compared to related works, this analysis is clearer. An NS2 simulation was developed, in which the experimental results show that the designed communication protocol is workable. Therefore, regardless of the security analysis, time complexity, and communication cost, our dynamic key management is an appropriate mechanism for wireless sensors network.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This research was supported by the National Science Council, Taiwan, under Contract nos. MOST 103-2632-E-324-001-MY3, MOST 103-2622-E-212-009-CC2, MOST 103-2221-E-324-023, and MOST 104-2221-E-324-012.

References

[1] C.-L. Chen, T.-F. Shih, Y.-T. Tsai, and D.-K. Li, "A bilinear pairing-based dynamic key management and authentication for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 534657, 14 pages, 2015.

[2] C.-L. Chen, Y.-T. Tsai, A. Castiglione, and F. Palmieri, "Using bivariate polynomial to design a dynamic key management scheme for wireless sensor networks," *Computer Science and Information Systems*, vol. 10, no. 2, pp. 589–609, 2013.

[3] Y. Cheng and D.-P. Agrawal, "An improved key distribution mechanism for large-scale hierarchical wireless sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 35–48, 2007.

[4] C.-L. Chen, Y.-Y. Chen, and Y.-H. Chen, "Group-based authentication to protect digital content for business applications," *The International Journal of Innovative Computing, Information and Control*, vol. 5, no. 5, pp. 1243–1251, 2009.

[5] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47, Washington, DC , USA, November 2002.

[6] Y. Cheng and D. P. Agrawal, "Efficient pairwise key establishment and management in static wireless sensor networks," in *Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '05)*, pp. 544–550, Washington, DC, USA, November 2005.

[7] D. Liu and P. Ning, "Improving key pre-distribution with deployment knowledge in static sensor networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 2, pp. 204–239, 2005.

[8] C. L. Chen and C. T. Li, "Dynamic session-key generation for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, Article ID 691571, 10 pages, 2008.

[9] C.-L. Chen and I.-H. Lin, "Location-aware dynamic session-key management for grid-based wireless sensor networks," *Sensors*, vol. 10, no. 8, pp. 7347–7370, 2010.

[10] C. Xu and W. Liu, "Key updating methods for combinatorial design based key management schemes," *Journal of Sensors*, vol. 2014, Article ID 134357, 8 pages, 2014.

[11] B. Zhou, J. Wang, S. Li, and W. Wang, "A new key predistribution scheme for multiphase sensor networks using a new deployment model," *Journal of Sensors*, vol. 2014, Article ID 573913, 10 pages, 2014.

[12] H.-F. Huang and W.-C. Wei, "A new efficient and complete remote user authentication protocol with smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 4, no. 11, pp. 2803–2808, 2008.

[13] C.-L. Chen, Y.-L. Lai, C.-C. Chen, and Y.-L. Chen, "A smart-card-based mobile secure transaction system for medical treatment examining reports," *The International Journal of Innovative Computing, Information and Control*, vol. 7, no. 5, pp. 2257–2267, 2011.

[14] C.-C. Chang and T.-C. Wu, "Remote password authentication with smart cards," *IEE Proceedings E: Computers and Digital Techniques*, vol. 138, no. 3, pp. 165–168, 1991.

[15] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[16] M. Kumar, "New remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 597–600, 2004.

[17] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[18] N. El-Fishway and A. Tadros, "An effective approach for authentication of mobile users," in *Proceedings of the IEEE 55th Vehicular Technology Conference*, vol. 2, pp. 598–601, 2002.

[19] C.-L. Chen, "An 'all-in-one' mobile DRM system design," *The International Journal of Innovative Computing, Information and Control*, vol. 6, no. 3, pp. 897–911, 2010.

[20] C.-M. Liu, C.-H. Lee, and L.-C. Wang, "Distributed clustering algorithms for data-gathering in wireless mobile sensor networks," *Journal of Parallel and Distributed Computing*, vol. 67, no. 11, pp. 1187–1200, 2007.

[21] M. Chatterjee, S. K. Das, and D. Turgut, "WCA: a weighted clustering algorithm for mobile ad hoc," *Cluster Computing*, vol. 5, no. 2, pp. 193–204, 2002.

[22] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Siences (HICSS '33)*, pp. 2–10, January 2000.

[23] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in *Proceedings of the 16th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '97)*, vol. 3, pp. 1405–1413, April 1997.

[24] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, February 1999.

[25] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, T. Imielinski and H. F. Korth, Eds., vol. 353, pp. 153–181, Springer, 1996.

[26] Crossbow Technology Inc, http://www.xbow.com/.

[27] C. Alcaraz, J. Lopez, R. Roman, and H.-H. Chen, "Selecting key management schemes for WSN applications," *Computers & Security*, vol. 38, no. 8, pp. 2257–2267, 2012.

[28] S. M. M. Rahman and K. El-Khatib, "Private key agreement and secure communication for heterogeneous sensor networks," *Journal of Parallel and Distributed Computing*, vol. 70, no. 8, pp. 858–870, 2010.

[29] Intel company, http://www.intel.com/content/www/us/en/homepage.html.

[30] Atmel company website: AVR 8-Bit RISC processor, http://www.atmel.com/products/.

[31] IEEE 802.15.4 Standard, http://www.ieee802.org/15/pub/TG4.html.