Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 913782, 8 pages
http://dx.doi.org/10.1155/2013/913782

Research Article

A Privacy-Preserving Reauthentication Scheme for Mobile Wireless Sensor Networks

Shunrong Jiang, Jiapeng Zhang, JingJun Miao, and Conghua Zhou

The Department of Internet of Things, Jiangsu University, Zhenjiang 212013, China

Correspondence should be addressed to Shunrong Jiang; jsywow@gmail.com and Conghua Zhou; chzhou@ujs.edu.cn

Received 1 March 2013; Revised 23 April 2013; Accepted 23 April 2013

Academic Editor: Liangmin Wang

The mobile wireless sensor network (MWSN) is a new style WSN with mobile sinks or sensors in the network. MWSN has advantages over static WSN in the aspect of better energy efficiency, improved coverage, and superior channel capacity. However, mobile nodes also bring some security problems. For example, it is difficult to ensure secure communications among the mobile nodes and static nodes. In this paper, we design a lightweight mobile reauthentication protocol for mobile nodes. The designed protocol provides forward secure pairwise key for the mobile node when it moves from one cluster to another. Thus, the mobile sensor node can be authenticated by the new cluster head, and the privacy of his origin area is protected. In addition, the security and performance analysis shows that our scheme meets the need of lower communication and computation overhead, while achieving security requirement for mobile sensor node application in MWSN.

1. Introduction

WSN has become more and more prospective in human life with the development of hardware and communication technologies. However, due to the static network style, there are some natural limitations of WSN, such as network connectivity and network lifetime [1–4]. Furthermore, more and more researches find that the mobility in WSN not only improves the overall network lifetime and the data capacity of the network, but also addresses delay and latency problems [5–9]. There are many researches on how to realize better energy efficiency, improve coverage, enhance target tracking, and cause superior channel capacity for MWSN. However, limited researches consider the issue caused by the mobile sensor nodes, such as credibility with low consumption overhead and secure communication in MWSN. While more and more application scenarios require mobile sensors in WSN, such as traffic detection, animal observation E-Health, and battlefield. Furthermore, some present researches begin to consider the mobile adversary [10], which brings new security problems. Therefore, we should pay attention to realize the mutual authentication between the mobile node and the cluster efficiently, generate the new pairwise key, and make sure of the security of data transmission.

The framework of MWNS is given as in Figure 1. The network considers four types of entities:

(1) base station—as usual, the base station is assumed to be absolutely secure, which has plenty bandwidth, energy, storage space, and computation capability;

(2) cluster head—cluster head is assumed to have more storage space, energy, communication range, and computation capability than sensor node, and notice that, in general, the communication range of cluster head is also larger than the sensor node;

(3) static sensor node—we consider static sensor nodes in our network model, since they can work for the cluster head, and relay for mobile sensor node which has smaller communication range than cluster head, and in general, we assume that it has limited storage space, energy, and communication range;

(4) mobile sensor node—the mobility is the only difference between the mobile sensor node and the static sensor node, and the mobile sensor node roams from one cluster to another cluster and communicates with the nodes in the cluster.

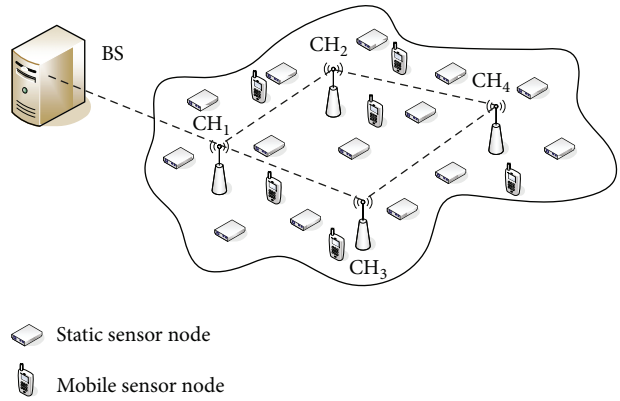

Figure 1: The framework of MWSN.

Based on the framework of MWSN, some security problems are brought by the mobility of mobile sensor node. One problem is the identity authentication of mobile sensor node in the new cluster. The other is the new session key generated between mobile sensor node and new cluster to ensure security communication. Moreover, we should protect the privacy of the mobile sensor node which means attackers cannot track it. Therefore, the security requirements of MWSN are given as follows:

(1) the authentication of identity—making sure that the identities of both parties who generate the key are trusted;

(2) data integrity—ensuring that only authorized person can modify the transmission of information;

(3) message privacy—transferring data can only be read by authorized parties;

(4) key freshness: ensuring that the existing session key is only used at current stage;

(5) node Resiliency—the network recovers when some nodes are captured by malicious attackers;

(6) privacy-preserving—since the mobile sensor node roams in WSN, attackers cannot track the mobile sensor node;

(7) scalability—allowing revoking and joining nodes. With the expanding of the network scale, it has little effect on the storage space of nodes and communication consumption.

In this paper, we focus on the security requirements caused by mobile sensor nodes. For the mobile sensor node in MWSN, we present an efficient node reauthentication and key generation scheme for mobile sensor nodes which consumes less communication and computation overhead and protects the privacy of the mobile sensor node. The security and performance analysis shows that our re-authentication scheme for mobile sensor node cannot only efficiently realize the secure requirements for MWSN, but also suit for the limited resource WSN.

The rest of this paper is organized as follows. In Section 2, we introduce the related work. We present our protocol in Section 3. Section 4 gives the security analysis of re-authentication protocol. Section 5 gives the performance analysis and simulation. Finally, we conclude the paper in Section 6.

2. Related Work

We introduce our related work from three aspects: the lightweight authentication schemes for WSN, the research of mobile sink in MWSN, and the re-authentication schemes for the mobile sensor node in MWSN.

The demand of lightweight is mostly considered in sensor network. All nodes in sensor network are considered to be static initially. For example, Perrig et al. [11] proposed a typical authentication scheme named μTESLA (Timed Efficient Stream Loss-Tolerant Authentication) by using the one-way hash chain. The protocol publishes the authentication key K_{mac} through delay to ensure that before the K_{mac} is published, the attacker cannot forge the correct broadcast packets. Du et al. [12] constructed an authentication path based on the public key mechanism by using Merkle Tree to reduce the computation and communication overheads. He also proposed dividing the entire WSN network into region Merkle Tree which can reduce the height of the Tree and the hops of the authentication. Ibriq and Mahgoub [13] proposed an efficient authentication program in which BS (Base Station) acts as the role of Certificate Authentication (CA) and assigns part of its functions to CH (Cluster Head). A sink can generate a key from "Partial Key Escrow Tab" [13] in all nodes and can be elected as Cluster Head. After the data integrated, messages are exchanged among cluster heads and finally transmitted to BS. However, since the partial key escrow Tab should be stored in every node, this scheme needs additional storage space. All these authentication protocols are for static nodes without considering roaming issue.

The advantages of mobile sink in MWSN have attracted much attention. Zhang et al. [14] proposed several efficient schemes to restrict the privilege of a mobile sink without impeding its capability of carrying out authorized operations for an assigned task. To prevent the authenticator from revealing information due to mobile sink compromises, the privileges of the authenticator are restricted by adding parameters, such as the starting time and the ending time of a task, the type of a task, and ID of the mobile sink. Vieira et al. [15] proposed a bioinspired location service named Phero-Trail location service protocol. In Phero-Trail, location information is stored in a 2D upper hull of a Sensor Equipped Aquatic Swarm, and a mobile sink uses its trajectory projected to the 2D hull to maintain location information. This enables mobile sensors to efficiently locate a mobile sink. The results show that Phero-Trail performs better than existing approaches. Agrawal et al. [16] proposed a key update protocol which securely updates the session key between a pair of nodes with the help of random inputs in mobile sensor networks. The security analysis shows that the proposed protocol resists known-key, impersonation, replay, worm, and sink hole attacks, while also provides forward secrecy, key freshness, and key control.

Table 1: Notation.

Notation	Description
T	Timestamp
M_A	The mobile node
CH_A, CH_B	The cluster head
$K_{A,B}$	The pair-wise key for A and B
$\{M\}_K$	Encrypt message M by K
$MAC(k, M)$	The message authentication code of M using K
$H()$	Hash function
$\|\|$	Message connecting
$\oplus$	Xor

Recently the security of mobile sensor nodes in WSN has been paid more and more attention. Han and Kim [17] proposed the re-authentication issue concerning mobile nodes moving among sink nodes. The scheme considers the sink in the home cluster as a trusted third party. It prestores authentication information in all surrounding neighbor clusters and transfers the credible information to the new sink. The communication and computation overhead of re-authentication is reduced through credible trust. Qiu et al. [18] considered a sensor node roaming within a very large and distributed wireless sensor network, such as the application of healthcare field, in which the sensor nodes are deployed in the patient's body. When a dynamic sensor node moves to new area and wants to attack a router or a cluster head in this area, it first sends a request message to the base station. After verifying validity of the request message, the base station generates the session key for mobile node and the router and sends it to the router, and then the router sends the material of session key to the mobile node to generate the session key. Qiu also improves the E-G scheme to guarantee that two sensor nodes share at least one key with probability 1 with less storage and energy overhead. The disadvantages of Han's scheme are as follows. First, it only takes the mobile node, sink node, and base station into consideration. Then, the communication overhead of the program mostly concentrates on the mobile node, so it has influence on the lifetime of the mobile node. Lastly, the re-authentication material is prestored in the neighbor clusters, which exists unnecessary communication overhead and information leak. In Qiu's scheme, the base-station is always online and provides the full utilities. The re-authentication also depends on the base station which incurs large communication overhead.

3. The Proposed Protocol

With the mobility of MWSN, the mobile sensor nodes may move from one cluster to another. If we repeat the new nodes addition process proposed in [4], the scheme will degrade to the E-G [19] scheme. Besides, some predistribution schemes need to interrupt the operation of network and implemented by man, which is unrealistic for the running wireless network. Therefore, the roaming behavior of mobile sensor nodes must consider how to get trust from the new cluster and generate the pair-wise key to achieve security communication. Considering the security requirements caused by mobile sensor nodes in the MWSN, we design our re-authentication protocol as follows. For convenience, we assume that after the static WSN generated the communication keys for the entities, the mobile sensor nodes join the network from some clusters.

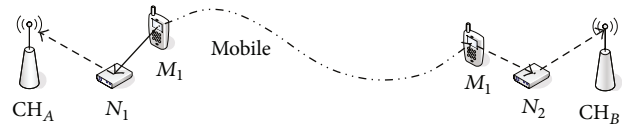

Figure 2: The re-authentication of mobile sensor node.

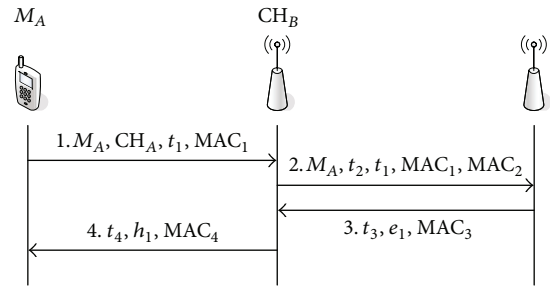

Figure 3: Re-authentication of mobile sensor nodes.

As Figure 2 shows, the whole process can be divided into two phrases. *Phrase 1* the mobile sensor node M_A first registers at the base station and then joins the network from the fixed cluster CH_A (home cluster). The main purpose of this phase is to make M_A initial trustily join the network. To ensure security, this phrase is realized by offline distribution. *Phrase 2* M_A moves to another new cluster CH_B (foreign cluster), and it should pass the legal identify authentication of CH_B before enjoying the resource of this cluster. To realize the mutual authentication of M_A and CH_B, we can use the trusted relationship among M_A, CH_A, and CH_B. We describe the further details of re-authentication as follows. The notation used throughout our scheme is shown in Table 1.

3.1. Predistribution for Mobile Sensor Node. Before roaming in the network, M_A should register in the base station and get the pre-distribution material by offline. Then, M_A joins the network from cluster head CH_A. After being authenticated by CH_A, M_A has the information including a hash number $H(I)$, a random number R_1, and the session key K_{CH_A,M_A}.

3.2. Mobile Sensor Node Reauthentication. After registering at the base station and trusted joining CH_A, M_A can roam in the network among clusters. As Figure 2 shows, after completing *Phase 1*, the mobile sensor node M_A moves to a foreign cluster CH_B, and M_A should pass the authentication of CH_B before communicating with other nodes in CH_B. The implementation mutual authentication of re-authentication protocol is shown in Figure 3.

Require: $M_A, t_2, t_1, \mathrm{MAC}_1, \mathrm{MAC}_2$.
1: Verify $(t* - t_2) \le \Delta t$.
2: **if** t_2 is valid **then**
3: Compute $\mathrm{MAC}_2* = (K_{\mathrm{CH}_B,\mathrm{CH}_A}, M_A||t_2||t_1||\mathrm{MAC}_1)$.
4: **if** $\mathrm{MAC}_2* = \mathrm{MAC}_2$ **then**
5: Compute $\mathrm{MAC}_1* = (K_{\mathrm{CH}_A,M_A}, M_A||t_1||H(I))$.
6: **if** $\mathrm{MAC}_1* = \mathrm{MAC}_1$ **then**
7: Compute $e_1 = \{H(I), R_1\}_{K_{\mathrm{CH}_A,\mathrm{CH}_B}}$ and $\mathrm{MAC}(K_{\mathrm{CH}_A,\mathrm{CH}_B}, t_3||e_1)$.
8: **end if**
9: **end if**
10: **end if**

Algorithm 1: The process executed by CH_A to *message 2*.

Require: t_3, e_1, MAC_3.
1: Verify $(t* - t_3) \le \Delta t$.
2: **if** t_3 is valid **then**
3: Compute $\mathrm{MAC}_3* = \mathrm{MAC}(K_{\mathrm{CH}_A,\mathrm{CH}_B}, t_3||e_1)$.
4: **if** $\mathrm{MAC}_3* = \mathrm{MAC}_3$ **then**
5: Extract $H(I)$ and R_1.
6: Generate random number R_2, compute K_{CH_B,M_A} as formula (1).
7: Compute $h_1 = H(R_1) \oplus R_2$.
8: Compute $\mathrm{MAC}_4 = (K_{\mathrm{CH}_B,M_A}, H(I)||t_4||h_1)$.
9: **end if**
10: **end if**

Algorithm 2: The process executed by CH_B to *message 3*.

(1) When M_A moves to the new cluster CH_B, it first launches the authentication procedure to CH_B. M_A sends *the message 1*: M_A, CH_A, t_1, MAC_1 to CH_B, where t_1 is the timestamp, and $\mathrm{MAC}_1 = (K_{\mathrm{CH}_A,M_A}, M_A||t_1||H(I))$.

(2) When CH_B receives *message 1* at time $t*$, and CH_B first checks whether $(t* - t_1) \le \Delta t$. If the result is valid, since there is no shared information between CH_B and M_A, and CH_B would send *message 2*: M_A, t_2, t_1, MAC_1, MAC_2 to CH_A, where $\mathrm{MAC}_2 = (K_{\mathrm{CH}_B,\mathrm{CH}_A}, M_A||t_2||t_1||\mathrm{MAC}_1)$.

(3) Upon Receiving the *message 2*, the home cluster CH_A verifies message as Algorithm 1 and replies *message 3*: t_3, e_1, MAC_3 to CH_B.

(4) After receiving the *message 3*, CH_B verifies message as Algorithm 2. Then, CH_B sends the *message 4*: t_4, h_1, MAC_4 to M_A.

(5) Upon receiving the *message 4* from CH_B, the mobile node M_A executes Algorithm 3 to get the pair-wise key

$$K_{\mathrm{CH}_B,M_A} = H\left(H\left(I\right)\left\|R_1\right\|R_2\right). \tag{1}$$

After generating the session key, M_A verifies the correctness of MAC_4. If the validation is right, the session key is right. During the communication with CH_B, $H(I)$ and R_1 should be updated as $H(I')$ and R_1' which are used as the authentication material for the further re-authentication. CH_B also sends these information to the base station.

For convenience, the role of home cluster is acted by the foreign cluster node through which the mobile sensor nodes have completed the re-authentication process. That means that after M_A completes re-authentication in the foreign cluster CH_B, CH_B is the new home cluster of mobile sensor node. When M_A moves to another foreign cluster CH_C, CH_B acts as the home cluster which responsibly completes the re-authentication between M_A and CH_C.

Taking the issue of tracking and protecting the privacy of M_A into account, we use the pseudonyms methods [20, 21] during the communication. The whole time of M_A in CH_B is divided in accordance with the time slice TS_j, and the length of each time slice is Δt, which means we can get C time slices. We denote $\mathrm{PID}_{A,j}$ as the pseudonym of M_A in the time slice TS_j, where $\mathrm{PID}_{A,j}$ is generated by two hash seeds $H(I)$ and R_2 as formula (2)

$$\begin{aligned} S_{1,j} &= H^j\left(R_2\right), \\ S_{2,j} &= H^j\left(H\left(I\right)\right), \\ \mathrm{PID}_{A,j} &= H\left(S_{1,j} \oplus S_{2,j}\right). \end{aligned} \tag{2}$$

Require: t_4, h_1, MAC_4.
1: Verify $(t* - t_4) \leq \Delta t$.
2: **if** t_4 is valid **then**
3: Compute $H(R_1)$, and $R_2* = h_1 \oplus H(R_1)$.
4: Compute $K_{\mathrm{CH}_B,M_A}*$ as formula (1).
5: Compute $\mathrm{MAC}_4* = (K_{\mathrm{CH}_B,M_A}*, H(I)||t_4||h_1)$.
6: **if** $\mathrm{MAC}_4* = \mathrm{MAC}_4$ **then**
7: $K_{\mathrm{CH}_B,M_A}* = K_{\mathrm{CH}_B,M_A}$.
8: **end if**
9: **end if**

Algorithm 3: The process executed by M_A to *message 4*.

Notice that since CH_B knows R_2 and $H(I)$, so it can trace the messages sent by M_A in its communication range. While M_A moves to CH_C at TS_j (actually CH_C only knows a mobile sensor node named $\mathrm{PID}_{A,j}$ joining its cluster), because CH_B does not have the materials to generate the pseudonyms, so it cannot trace the messages sent by M_A out of its communication range. By this way, we can protect the privacy of M_A.

4. Protocol Security Analysis

4.1. The Protocol Satisfies Forward Security. Suppose that the attacker gets the session key K_{CH_C,M_A} between the mobile sensor node M_A and cluster node CH_C. It is difficult for attackers to derive the session key used before such as K_{CH_B,M_A}. The session key between M_A and CH_B is determined by two random numbers R_1 and R_2. R_1 is produced in the last reauthentication cycle and is transmitted in the ciphertext. R_2 is transmitted by the XOR hash value h_1 in *message 4*. If the attacker wants to obtain the plaintext R_1, he must know the session key K_{CH_A,M_A} between M_A and CH_A. Thus, the problem is deduced into how to get the session key between M_A and the first cluster CH_A. K_{CH_A,M_A} is sent offline, which is assumed to be secure. R_2 is gotten by the hash and XOR of the hash value of R_1, and according to the irreversibility of hash, the problem of obtaining the plaintext of R_2 is derived to obtain the plaintext R_1. Even if attackers get the current session key of M_A, they cannot derive the previous session key of M_A through the previously analysis. The protocol satisfies forward security.

4.2. Mutual Identity Authentication. In our scheme, as there is no shared information between CH_A and CH_B, CH_B cannot verify the identity of M_A, so when CH_B receives *message 1*, it transfers the message to CH_A. CH_A helps CH_B authenticate the identity of M_A by computing MAC_1 through using the hidden $H(I)$. M_A authenticates the identity of the foreign cluster CH_B mainly through MAC_4 which also uses the hidden $H(I)$. If MAC_4 is right, we believe that CH_B has the right identity. By this way, we realize mutual identity authentication.

4.3. Prevent Man-in-the-Middle Attack. From the analysis of our scheme, an attacker can track or intercept *message 1* to act the mobile sensor node M_A and continue communicating with foreign cluster head. It makes the entire protocol go on running. Finally, feedback message (*message 4*) is gotten to extract the session key material. However, according to the analysis of forward security, R_1 and R_2 are not sent in plaintext. In order to attack the protocol, the previous session key should be known. And the whole problem is back to the security of K_{CH_A,M_A}. For man-in-the-middle attack, as mentioned in mutual identity authentication, mutual identity authentication ensures the correctness of the identity of the message sender. MAC used in every message ensures the message integrity. According to the general security assumption of MAC [17], attackers cannot construct a valid message to achieve communication. So the protocol can prevent man-in-the-middle attack.

4.4. Prevent Replay Attack. When the mobile node M_A applies to join registered foreign cluster, every message of our scheme has the current timestamp (t_1, t_2, t_3, t_4). The message received in Δt time, to some extent, can prevent replay attack. According to the session key generated in formula (1), the generation of session key selects new random number, which ensures the freshness of session key and prevents replay attack effectively.

4.5. Protect the Privacy of the Mobile Node. Since the communication of mobile sensor node uses the pseudonyms, attackers and other entities cannot distinguish them which protects the privacy of the mobile sensor node. But to the base station and cluster heads, they can track the mobile sensor node. After the mobile node joins the foreign cluster, the cluster head sends the $H(I)$ and R_1 to the base station, which helps the base station to track and manage the mobile sensor node. However, for the cluster head (such as CH_C), CH_C only knows that the pseudonyms of the mobile sensor node M_A is in its cluster. When the mobile sensor node M_A moves to a new cluster head (such as CH_D), CH_C does not know the pseudonyms of M_A, and it cannot track M_A. Therefore, the privacy preserving of mobile sensor node is conditional.

5. Protocol Performance Analysis

We give the performance analysis of our scheme in this section in terms of communication pass, message size, and

Table 2: The required number of communication passes.

	Han's scheme	Qiu's scheme	Our scheme
Node to Sink	$2n$	n	n
Sink to Sink	m	l	2
Sink to Node	1	1	1
BS to Sink	—	1	—

computation overhead. We also give the simulation of our scheme on the NS2 simulation platform and use the time delay to reflect the efficiency of our scheme.

5.1. Communication Pass. We compared the required number of communication passes with Han's [17] and Qiu's [18] schemes, since both of them propose the reauthentication protocols for mobile sensor nodes in WSN. Table 2 shows the comparison of communication passes for mobile node reauthentication, where n denotes the number of hops from M_A to the foreign cluster head (sink), m denotes the number of neighbor cluster heads (sinks) around the home cluster head, and l denotes the number of hops from foreign cluster (sink) to the base station which is used in Qiu's scheme.

Since Han's and our schemes use the relation among cluster heads to realize re-authentication for mobile sensor node, which do not need communication with the base station, in Qiu's scheme, when the node joins a new sink, it first sends the requirement message to the base station. Actually, the message is first sent to the foreign cluster head (n hops) and then to the base station via the foreign cluster (l hops) which incurs large communication overhead. The hole communication passes are $(n + l)$ hops.

Although the re-authentication of Han's scheme does not need communication with the base station, he pre-stores the authentication information in all surrounding neighbor cluster heads which are related with the number of neighbor cluster (m hops), while our scheme realizes the re-authentication by the tradition tripartite authentication, which results in less communication pass.

5.2. Message Size. The message size during the re-authentication process is quantified by the byte which is to show the communication overhead. We compare the message size with Han's. We use the base parameter setting of message as Han's [17] in Table 3.

From Table 4, we can see that our scheme has less message size of the whole re-authentication process. Notice that Han pre-stores authentication information in all surrounding neighbor clusters and we only consider that the number of authentication material of transmission size is 36 bytes, while the actual number may be more than 36.

During re-authentication for mobile sensor node, we reduce the message length transmission among the entities since the data transmission consumes much more energy than computation in WSN.

5.3. Computation Overhead. Computation overhead is quantified by the number of execution encryption algorithm. As Table 5 shows, the total number of encryption/decryption of our scheme is the same as Han's, both more than Qiu's scheme. Since the re-authentication of Qiu's scheme is based on the base station, our scheme and Han's scheme are based on the relation among clusters.

Table 3: The base parameter setting of message.

Notation	Length (byte)
MAC	4
Random number	8
Identity	1
Time stamp	8
Key size	16

Table 4: The required message size for re-authentication (byte).

	Han's scheme	Qiu's scheme	Our scheme
Node to Sink	$48n$	$15n$	$14n$
Sink to Sink	$\geq 36m$	$15l$	53
Sink to Node	86	22	20
BS to Sink	—	50	—
Total	$\geq (48n + 36m + 86)$	$15(n + l) + 72$	$14n + 73$

Table 5: The required message size for re-authentication.

	Han's	Qiu's	Ours
Encryption/decryption in total	4	2	4
Encryption/decryption in node	1	1	2
MAC generation/verification in total	8	4	8
MAC generation/verification by node	3	2	4

5.4. Protocol Simulation. We use NS2.29 to simulate our scheme and Han' scheme [17], since both of them realize mobile node re-authentication without requiring communication with the base station. We use the transmission delay to quantify the message size, which can reveal the availability and efficiency of our scheme. The simulation uses the mesh network topology, MAC layer uses the 802.15.4 protocol written by Zheng and Lee [22] for NS2, the routing layer uses the AODV routing protocol which has the shortest hops, the transportation layer uses the UDP protocol, and the application layer transmits the CBR packet. The message size is set as Table 4. The data transmission speed is 250 KB/S, which adopts the recommended beacon mode standard setting in reference [22].

Supposing the communication radius of the mobile sensor node and the common sensor nodes within the cluster to be 20 m, the communication radius of cluster head is 100 m. The computation delay of *message 1* and *message 4* in mobile sensor node is 6 ms and 3 ms [23], respectively, while the computation delay of *message 2* and *message 3* node is 1 ms for cluster head.

To reflect the comparison of Table 4, we design two groups of simulation for our scheme and Han's scheme [17]. The number of each group simulation is 100 times.

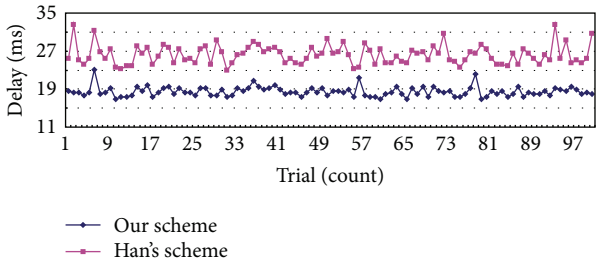

Figure 4: The time delay for $m = 1$, $n = 2$.

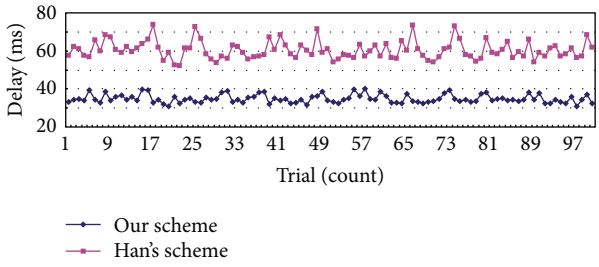

Figure 5: The time delay for $m = 1$, $n = 5$.

In Figure 4, $m = 1$, and $n = 2$. The simulation delay of Han's scheme is 26.217 ms, while our scheme is 18.432 ms. However, the time delay of our schemes simulation is not as good as the comparison in Table 4. Since there is an addition MAC layer head for each message, the time delay of simulation is not the same as the comparison of message size in Table 4. From Figure 4, we can know the whole delay of our scheme is less than Han's. On one hand, our scheme has less message size, on the other hand, we reduce the number of messages sending. The fluctuation of the simulation in Figure 4 is caused by $n = 2$. Since the message transmitted by the static nodes in cluster needs to consume transmission delay (when node transmits message, it will repeat calling the sending and receiving process, and seek the routing table, which leads to more delay time), and it results in the unstability of time.

In Figure 5, $m = 1$, and $n = 5$. The simulation delay of Han's scheme is 60.384 ms, while our scheme is 34.8608 ms. Compared with Figure 4, with the number of relay hops increasing, the advantage of our scheme is more obvious. This is due to less communication message size of mobile sensor node. Moreover, with the number of hops increasing, the instability of the simulation is more obvious.

6. Conclusion

The security problem brought by the mobile sensors in MWSN attracts more and more attention of researchers. In this paper, we propose a re-authentication protocol for the mobile node roaming among clusters. Our protocol can transfer the credibility among the clusters which can efficiently achieve the requirements of secure identity authentication and establish the forward secure pairwise key. Meanwhile, the base station can track the mobile trajectory and protect the privacy of the mobile sensor node. We also give performance analysis and simulation for our re-authentication protocol. The results and comparison show that our protocol achieves better security and has better performance on communication overhead, message size, and computation cost.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61202474 and the Natural Science Foundation of Jiangsu Province under Grant BK2011464.

References

[1] M. F. Younis, K. Ghumman, and M. Eltoweissy, "Location-aware combinatorial key management scheme for clustered sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 8, pp. 865–882, 2006.

[2] M. Eltoweissy, M. H. Heydari, L. Morales, and I. H. Sudborough, "Combinatorial optimization of group key management," *Journal of Network and Systems Management*, vol. 12, no. 1, pp. 33–50, 2004.

[3] S. Hussain, F. Kausar, and A. Masood, "An efficient key distribution scheme for heterogeneous sensor networks," in *Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC '07)*, pp. 388–392, New York, NY, USA, August 2007.

[4] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 24–34, 2007.

[5] S. A. Munir, B. Ren, W. Jiao, B. Wang, D. Xie, and J. Ma, "Mobile wireless sensor network: architecture and enabling technologies for ubiquitous computing," in *in Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, pp. 113–120, Niagara Falls, Canada, 2007.

[6] M. Rahimi, H. Shah, G. S. Sukhatme, J. Heideman, and D. Estrin, "Studying the feasibility of energy harvesting in a mobile sensor network," in *Proceedings of the IEEE International Conference on Robotics and Automation (ICRA '03)*, pp. 19–24, September 2003.

[7] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting heterogeneity in sensor networks," in *Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies (NFOCOM '05)*, pp. 878–890, Hillsboro, Ore, USA, March 2005.

[8] W. Wang, V. Srinivasan, and K. Chua, "Using mobile relays to prolong the lifetime of wireless sensor networks," in *Proceedings of the 11th Annual International Conference on Mobile Computing and Networking (MobiCom '05)*, pp. 270–283, New York, NY, USA, 2005.

[9] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '05)*, pp. 300–308, New York, NY, USA, May 2005.

[10] R. D. Pietro, C. Soriente, A. Spognardi, and G. Tsudik, "Collaborative authentication in unattended wsns," in *Proceedings of the*

2nd ACM Conference on Wireless Network Security (WiSec '09), pp. 237–244, New York, NY, USA, 2009.

[11] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

[12] W. Du, R. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks," in *Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing (MobiHoc '05)*, pp. 58–67, New York, NY, USA, 2005.

[13] J. Ibriq and I. Mahgoub, "A hierarchical key establishment scheme for wireless sensor networks," in *Proceedings of the 21st International Conference on Advanced Information Networking and Applications (AINA '07)*, pp. 210–219, NiagaraFalls, Canada, May 2007.

[14] W. Zhang, H. Song, S. Zhu, and G. Cao, "Least privilege and privilege deprivation: Towards tolerating mobile sink compromises in wireless sensor networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '05)*, pp. 378–389, New York, NY, USA, May 2005.

[15] L. F. M. Vieira, U. Lee, and M. Gerla, "Phero-trail: a bio-inspired location service for mobile underwater sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 4, pp. 553–563, 2010.

[16] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopes, "A novel key update protocol in mobile sensor networks," in *Proceedings of the 8th International Conference on Information Systems Security (ICISS '12)*, vol. 7671 of *Lecture Notes in Computer Science*, pp. 194–207, 2012.

[17] K. Han and K. Kim, "Untraceable mobile node authentication in wsn," *Sensors*, vol. 10, pp. 4410–4429, 2010.

[18] Y. Qiu, J. Zhou, J. Baek, and J. Lopez, "Authentication and key establishment in dynamic wireless sensor networks," *Sensor*, vol. 10, pp. 3718–3731, 2010.

[19] L. Eschenauer and V. Gligor, "A key management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)*, pp. 41–47, New York, NY, USA, 2002.

[20] S. Jiang, X. Zhu, and L. Wang, "A conditional privacy scheme based on anonymized batch authentication in vehicular ad hoc networks," in *Proceedings of the Wireless Communications and Networking Conference (WCNC '13)*, Shanghai, China, 2013.

[21] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.

[22] J. Zheng and M. Lee, "A comprehensive performance study of IEEE 802.15.4," in *Proceedings of the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB '08)*, pp. 580–585, 2008.

[23] G. D. Meulenaer, F. Gosset, F. X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *Sensor Network Operations*, chapter 4, pp. 218–237, Wiley-IEEE Press, New York, NY, USA, 2006.