An Efficient Authentication Scheme Based on Deployment Knowledge Against Mobile Sink Replication Attack in UWSNs

Boqing Zhou, Sujun Li, Weiping Wang, *Member, IEEE*, Jianxin Wang, *Senior Member, IEEE*, Yun Cheng, and Jie Wu, *Fellow, IEEE*

***Abstract*—Unattended wireless sensor networks (UWSNs) are vulnerable to mobile sink (MS) replication attack. In this attack, using the compromised key information, an attacker can collect data from networks by impersonating sinks. To resist such an attack, some schemes have been proposed. To improve the resilience of MS replication attack of these schemes, we can integrate them with schemes based on deployment knowledge. However, there are the following defects: 1) the probability of mutual authentication between a MS and a sensor node is less than 1 and 2) during the authentication phase, the energy consumption of sensor nodes increases significantly as the deployment area expands. In this paper, we construct 3-D backward key chains based on deployment knowledge and propose a new authentication scheme based on these. As compared with these existing related schemes, the detailed theory analysis and simulation results indicate that the scheme can ensure that a MS can be authenticated by sensor nodes, and can improve the resilience of networks' MS replication attack with low energy consumption.**

***Index Terms*—3-D backward key chain based on deployment knowledge, authentication, mobile sink (MS) replication attack, unattended wireless sensor networks (UWSNs).**

I. Introduction

Wireless sensor networks (WSNs) usually consist of a large number of ultrasmall autonomous sensors. WSNs are being deployed for a wide variety of applications [1], including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc. Many WSNs are assumed to operate in real-time mode wherein, soon after acquiring data, sensor nodes send it to a trusted sink. There are also other applications that do not fit into the real time data collection model. Consider an example of a monitoring system deployed along an international border to record illegal crossings. The size of the surveillance area would require a mobile sink (MS) to collect data periodically [2]. We refer to such networks as unattended WSNs (UWSNs) [2]–[5].

When UWSNs are deployed in a hostile environment, security becomes extremely important as they are prone to different types of malicious attacks [6]–[11], such as MS replication attack. To resist such an attack, authentication and pairwise key establishment between sensors and MSs are very important [6]–[11]. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a nontrivial task.

Public-key operations (both software and hardware implementations), albeit computationally feasible, consume energy approximately three orders of magnitude higher than symmetric key encryption [12]. Therefore, in the last few years, different key distribution schemes using symmetric key algorithms have been developed for WSNs [8]–[11], [13]–[28].

A. Motivation

In UWSNs, an MS is in charge of collecting data from sensor nodes sporadically. Therefore, UWSNs are vulnerable to MS replication attack [6]–[11]. In this paper, if a replication device can successfully collect data from sensor nodes in the network, then it is regarded as MS replication attack.

For heterogeneous sensor networks, Li *et al.* [9] proposed a secure scheme based on a master–slaver model, and an EQ method. In the proposed scheme, when there are a few nodes captured in the bootstrap phase, the security analysis and simulation indicate that it can provide a very good performance in networks' resilience against H-sensors replication attack.

However, in [9], the authentication between a sensor node and an H-sensor requires the cooperation of multiple H-sensors to complete. In UWSNs, the data of the entire network is generally collected by an MS. If the method in [9] is

Manuscript received March 23, 2019; revised June 15, 2019; accepted July 14, 2019. Date of publication July 24, 2019; date of current version December 11, 2019. This work was supported in part by the Research Foundation of Education Committee of Hunan Province, China, under Grant 16A110, in part by the National Natural Science Foundation of China under Grant 61672543, Grant 61772559, and Grant 61571188, in part by the Construct Program of the Key Discipline in Hunan Province, China, in part by the Aid Program for Science and Technology Innovative Research Team in Higher Educational Institute of Hunan Province, China. *(Corresponding authors: Boqing Zhou; Weiping Wang.)*

B. Zhou is with the School of Information Science and Engineering, Shaoguan University, Shaoguan 512005, China, and also with MOE-LCSM, School of Mathematics and Statistics, Hunan Normal University, Changsha, Hunan 410081, China (e-mail: zbq_paper@163.com).

S. Li is with the School of Information Science and Engineering, Shaoguan University, Shaoguan 512005, China (e-mail: lsj_paper@163.com).

W. Wang and J. Wang are with the School of Information Science and Engineering, Central South University, Changsha 410083, China (e-mail: wpwang@mail.csu.edu.cn; jxwang@mail.csu.edu.cn).

Y. Cheng is with the Department of Information, Hunan University of Humanities, Science and Technology, Loudi 417000, China (e-mail: chy8370002@gmail.com).

J. Wu is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122 USA (e-mail: jiewu@temple.edu).

Digital Object Identifier 10.1109/JIOT.2019.2930823

directly applied in UWSNs, a large number of sensor nodes will be wasted because they cannot authenticate the MS. In [10], a three-layer communication model integrated with q-scheme [14] and key space scheme [15] is presented. In this model, only with the help of static access sensors, an MS can establish a pairwise key with a sensor node. As a result, if sensor nodes compromised, replication MSs can collect data from UWSNs by impersonating static access nodes. To improve UWSNs' resilience against MS replication attack, Li *et al.* [11] proposed a scheme using joint authentication of neighbor nodes. However, in the scheme, these compromised neighbor nodes can cause DoS attack by jointly sending forged authentication information.

In addition, in WSNs, existing researches show that schemes based on deployment knowledge can significantly improve the security performance of the entire network [16]–[20]. In these schemes, the entire network is divided into multiple cells, each cell has a local key pool, and only these local key pools of adjacent cells share some common keys. That is to say, the number of keys in the global key pool, which is composed of all local key pools in the network, will increase significantly with the expansion of the deployment area. Zhou *et al.* [21], in order to improve the robustness to deployment errors, proposed a layer key management model and created 3-D backward key chains to implement this model. In this model, each cell still has a local key pool, but uses 3-D backward key chains to achieve keys sharing between a cell and its T-layer association cells. In UWSNs, an MS needs to predistribute more keys from the global key pool to ensure high-probability of being authenticated by nodes in the network. However, if these schemes which can resist MS replication attack [9], [11] are directly integrated with these schemes based on deployment knowledge, then the number of predistribution keys of an MS will increase with the expansion of the deployment area. As the number of predistribution keys of an MS increases, the amount of information that needs to be exchanged between an MS and a sensor node increases during the process of authentication. As a result, the energy consumption of sensor nodes will significantly increase. Obviously, in UWSNs, the problem of based on deployment knowledge to efficiently improve the resilience of MS replication attack remains unresolved.

B. Main Contribution of Our Scheme

To improve networks' resilience against MS replication attack, in this paper, we construct new 3-D backward key chains based on deployment knowledge and propose an authentication scheme based on this for UWSNs. The main contributions of this paper are as follows.

1) 3-D backward key chains based on deployment knowledge are constructed. And a global key pool based on these key chains is developed. The size of the global key pool is independent of the size of the deployed area. As a result, the number of keys predistributed to an MS is independent of the size of the deployed area. That is, during the authentication phase between an MS and a sensor node, the energy consumption of the sensor node does not increase with the expansion of the deployment area.
2) In our scheme, a new authentication mechanism between an MS and a sensor node is presented. In this scheme, the probability of successful authentication between an MS and a sensor node is 1. By dynamically adjusting the number of keys required for mutual authentication between an MS and a sensor node at different phases, it not only can reduce the energy consumption of sensor nodes, but also can improve networks' resilience against MS replication attack as compared with existing related schemes.

C. Organization

The rest of this paper is organized as follows. At first, the background of our scheme is presented in Section II. Subsequently, the notations and deployment knowledge and threat models used in this paper are presented in Section III. The proposed scheme will be presented in Section IV. Together with a comprehensive comparison with a known scheme, the theoretical and experimental results will be described in Section V. At last, the conclusion will be made in Section VI.

II. Related Work

The first key predistribution scheme is proposed by Eschenauer and Gligor [13] (E-G scheme), in which a large key pool P is computed offline, and each sensor node picks m keys randomly from P without replacement before deployment. Two sensor nodes can establish a shared key, as long as they have at least one key in common. To enhance the security of the E-G scheme against small-scale attacks, Chan *et al.* [14] proposed the q-composite keys scheme (q scheme), in which q ($q > 1$) common keys are required for two sensors to establish a shared key. This scheme performs worse in resilience when the number of compromised sensors is large. Ren *et al.* [22] and Bechkit *et al.* [23] used 1-D key chains and Hash chains to improve the performance of the E-G schemes and q scheme, respectively. However, these schemes do not consider the security throughout the lifecycle of networks. Rasheed and Mahapatra [8] proposed a pairwise key establishment scheme for UWSNs, which is the combination of the polynomial-pool-based key predistribution scheme [27], the probabilistic generation key predistribution scheme [28], and the q scheme [14]. Comparing it with the q-composite scheme, the probabilistic key predistribution scheme, and the polynomial-pool-based scheme, it performs better in terms of network resilience to node capture attack in UWSNs. Li *et al.* [24] and Zhou *et al.* [25], [26] used independent and interrelated key pools to improve networks' security throughout their lifecycle.

To improve the performance of key establishment, Du *et al.* [16] and Yu and Guan [17] proposed a scheme using predeployment knowledge, respectively. In [16], the target is divided into square cells. In [17], the target is divided into hexagon cells. Fanian *et al.* [18] redivided hexagonal cells, and proposed three key management models. These schemes can improve the performance of the scheme in [17] when deployment error is small. In these schemes, networks security throughout their lifecycle is not taken into account. Zhou *et al.* [19] proposed a scheme ESPK based on the combination of 1-D key chains and deployment knowledge [16]. The scheme can provide high network security throughout their lifecycle. However, local connectivity of the scheme ESPK decreases with the increase of the number of the deployment phase. The above deficiency is improved by the scheme proposed in [20]. For applications with large deployment errors, Zhou *et al.* [21] proposed a layer model. In this model, each cell is a basic cell, each basic cell has T-layer association cells which are around it, and shared keys between a basic cell and its T-layer association cells are realized by using 3-D backward key chains. This model not only applies to existing schemes [16]–[20], but also can improve these schemes' performance when deployment error is large. In these above schemes, each deployment cell has a local key pool whose size is fixed. As a result the number keys of the global key pool will increase with the expansion of the deployment area.

To improve networks' resilience against H-sensors replication attack, in [9], a master–slaver model, and an EQ method are proposed. In this scheme, a sensor node randomly selects EQ keys from its predistribution keys as authentication keys with its cluster head. This scheme can provide good resilience of replication attack. However, the probability of authentication between an H-sensor and a sensor node is low. If this scheme is directly applied to UWSNs, the data of many sensor nodes in the network cannot be collected by an MS because they cannot authenticate the MS. To improve networks' resilience against MS replication attack, in [10], a three-tier authentication scheme is proposed. In the three-tier authentication scheme, authentication between an MS and a sensor node is accomplished with the help of static access nodes, which makes an adversary easily know a great deal of key information of the static polynomial pool by capturing a small fraction of sensor nodes. As a result, the adversary can collect data from sensor nodes by launching static access node replication attack. Li *et al.* [11] proposed a (M, m) authentication scheme. In the scheme, a sensor node randomly chooses M neighbors to form its candidate authentication set and requires nodes in the candidate set to send key information for authentication to it. In the authentication process, a sensor node requires its candidate authentication nodes to send the authentication information to the MS. When the number of correct authentication messages received by the MS is not less than m, the MS can pass the authentication of the sensor node. The (M, m) authentication scheme can significantly improve the resilience of MS replication attack of two schemes [9], [10]. However, these compromised neighbor nodes can cause DoS attack by jointly sending forged authentication information. In addition, if these schemes [10], [11] are integrated with the schemes based on deployment knowledge, then the number of predistribution keys of an MS will increase with the expansion of the deployment area. As the number of predistribution keys of an MS increases, the amount of information that needs to be exchanged between the MS and a sensor node increases during the process of authentication. As a result, the energy consumption of sensor nodes will significantly increase. At the same time, the probability that a sensor node can correctly authenticate an MS is less than 1. Therefore, in UWSNs, it is important to develop a new key generation technology to ensure that the number of predistribution keys of an MS is independent of the size of the deployment region, and propose a new authentication technology based on this.

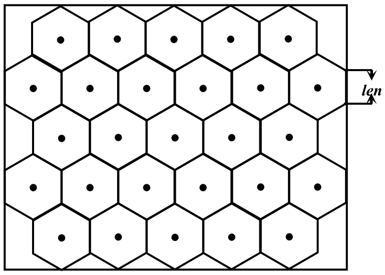


Fig. 1. Target field is partitioned into hexagon grids. • represents a deployment point.

III. Notations and Deployment Knowledge and Threat Models

A. Notations

In this paper, we use the following notations in Table I for the description convenience.

B. Deployment Knowledge Model

In this paper, we assume that a UWSN consists of a large number of static sensor nodes and an MS. The sensor nodes' deployment model is similar to [19]. As shown in Fig. 1, a target field is partitioned into hexagon cells, and each cell has a deployment point that resides in the center of the cell. Node distribution follows 2-D Gaussian distribution with the deployment point as the center.

Nodes deployed in the same cell form a group. Nodes deployed in the cell l are denoted by G_l. G_l is clustered into phases according to the deployment phase. The i-phase subgroup of G_l is denoted by G_l^i. In our scheme, SN_l represents the set of uncaptured nodes whose deployment points locate in the cell l (several schemes have been proposed to identify the compromised sensors in prior studies, such as [30] and [31]). When $|SN_l|$ is less than the threshold ρ, we should add new nodes to the cell.

C. Threat Model

The model for adversaries' capture is similar to [15]. In this model, an adversary intrudes on a cell and randomly captures and compromises sensor nodes whose deployment points locate in this cell. In the paper, we assume that an adversary randomly selects a cell and continuous to compromise nodes resides in the cell. Also, we suppose that captures occurring between the ith deployment phase and the $(i+1)$th deployment phase are called the ith time capture. If an attacker captures a sensor node, all key information it holds will also be compromised. Moreover, an adversary may pool the keying materials from multiple compromised nodes to break the security of the network or to launch advanced attacks, such as eavesdropping, MS replication attack [9], etc.

TABLE I
NOTATIONS USED

Notation	Description
len	The length of a hexagon cell
G_l	A group whose deployment point locates in a cell *l*
G_l^i	The i^{th} phase subgroup of G_l
a_l^i	A node of the G_l^i
$ID_{a_l^i}$	Identification of a_l^i
n	The number of deployment phase
R	Transmission radius of sensor nodes and mobile sinks
σ	Standard deviation of two-dimension Gaussian distribution
NC_l	Neighboring cells set of the cell *l*
H()	A one-way hash function
H_K()	A one-way hash function with the key *K*
|S|	The size of the set S
L	The total number of cells of the deployment area
L'	The length of the third-dimension key chain of a three-dimension backward key chain based on deployment knowledge
PG	Global key pool
PLG_l^i	The i^{th} phase of generation key pool of the cell *l*
PLC_l^i	The i^{th} phase of ordinary key pool of the cell *l*
t1	The number of generation keys pre-distributed to a sensor node
t2	The number of ordinary keys pre-distributed to a sensor node
t3	The number of keys pre-distributed to a mobile sink
BQ	The minimum number of common keys required for mutual authentication between an MS and a sensor node
AQ	A increment in the number of common keys for mutual authentication between an MS and a sensor node when the deployment phase increases by 1
SQ	The number of common keys required for mutual authentication between an MS and a sensor node
M_g	The maximum increment of phase during mutual authentication between an MS and a sensor node
DC_g	The maximum of deployment phase of sensor nodes in the network
T	The minimum of common keys between an MS and a sensor node
||	Concatenation operation
min(*d1*,*d2*)	Evaluation of the minimum of *d1* and *d2*
max(*d1*,*d2*)	Evaluation of the maximum of *d1* and *d2*

IV. OUR SCHEME

Based on deployment knowledge and threat models described in Section III, we propose an efficient authentication scheme for UWSNs. Our scheme includes the following two phases: 1) key predistribution phase and 2) pairwise key establishment and authentication phase.

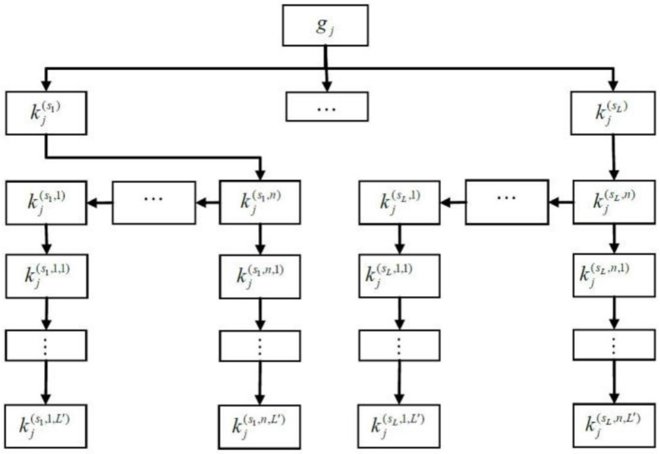


Fig. 2. 3-D backward key chain based on deployment knowledge.

A. 3-D Backward Key Chains Based on Deployment Knowledge

It is assumed that the total number of cells of the deployment area is *L*, and each cell has a unique ID $S_l (1 \le l \le L)$.

As shown in Fig. 2, the method for constructing a 3-D backward key chain based on deployment knowledge, namely C_j, is as follows.

1) The first dimension key chain, whose length is *L*, is generated by using a keyed hash function, namely $H_k(inf)$, as follows:

$$k_j^{(s_l)} = H_{g_j}(s_l), \text{ where } 1 \le l \le L \tag{1}$$

where g_j and $k_j^{(s_l)}$ represent the generation key of the 3-D backward key chain and the generation key of the cell S_l, respectively.

2) The second dimension key chain, whose length is *n*, is generated by using a hash function, namely $H(inf)$, as follows:

$$k_j^{(s_l,i)} = H\left(k_j^{(s_l,i+1)}\right), \text{ where}$$
$$k_j^{(s_l,n)} = H(k_j^{(s_l)}), \text{ and } i \in [1, n-1] \tag{2}$$

where $k_j^{(s_l,i)}$ represents the *i*th generation key of the cell S_l.

3) The third dimension key chain, whose length is L', is generated by using a keyed hash function, namely $H_k(inf)$, as follows:

$$k_j^{(s_l,i,l')} = H_{k_j^{(s_l,i)}}\left(k_j^{(s_l,i,l'-1)}\right), \text{ where}$$
$$k_j^{(s_l,i,1)} = H_{k_j^{(s_l,i)}}\left(k_j^{(s_l,i)}\right), \text{ and } 2 \le l' \le L' \tag{3}$$

where $k_j^{(s_l,i,l')}$ represents the (l')th key of the *i*th generation key of the cell S_l.

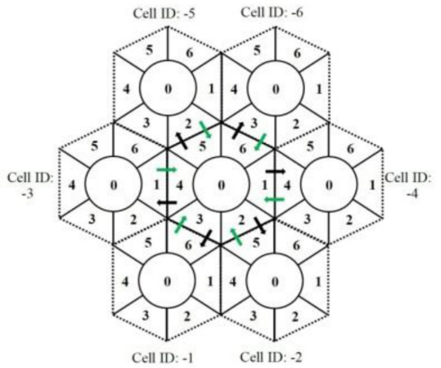


Fig. 3. Generation key pool of cell 1.

B. Key Pool

In our scheme, the number of 3-D backward key chains based on deployment knowledge is m. Key pools include a global key pool, namely $PG = \{g_j, 1 \le j \le m\}$, and local key pools based on cells, namely PL. A local key pool of a cell l, namely PL_l, is divided into n phases. PL_l^i represents the ith phase of PL_l, which includes the following two parts: 1) a local ordinary key pool, namely $PLC_l^i = \{k_j^{(l,i,l')} | 1 \le j \le m, 1 \le l' \le L'\}$ and 2) a local generation key pool, namely PLG_l^i. Next, the method for constructing PLG_l^i is described.

For a cell l, keys in $LG_l^i = \{k_j^{(l,i)} | 1 \le j \le m\}$ are separated into seven equal parts, a part is denoted by $(LG_l^i)_x$ $(0 \le x' \le 6)$. All $(LG_l^i)_x$ are ordered according to the method presented in Fig. 3. Then these neighbor cells exchange their $(LG_l^i)_x$ with each other. For example, cell 1 gives $(LG_1^i)_1$ to cell -4, cell -4 gives $(LG_{-4}^i)_4$ to cell 1. So, we can have

$$\begin{aligned}PLG_1^i = {} & \left(LG_1^i\right)_0 \cup \left(LG_{-4}^i\right)_4 \cup \left(LG_{-2}^i\right)_5 \cup \left(LG_{-1}^i\right)_6 \\ & \cup \left(LG_{-3}^i\right)_1 \cup \left(LG_{-5}^i\right)_2 \cup \left(LG_{-6}^i\right)_3.\end{aligned}$$

C. Key Predistribution Phase

A sensor node a_l^i $(a_l^i \in G_l^i)$ is preloaded with $t1$ and $t2$ $(t2 >> t1)$ keys along with these keys' IDs, from PLG_l^i and PLC_l^i, respectively. An MS only randomly picks keys from PG. The composition of PG indicates that the size of PG is independent of the size of deployment area. In this paper, An MS is preloaded with $t3$ $(t3 = m + T - t1 - t2)$ keys along with these keys' IDs, from PG.

D. Pairwise Key Establishment and Authentication Phase

In UWSNs, secure communications between two sensor nodes is achieved by establishing a pairwise key, and between a sensor node and an MS is achieved after authenticating each other. The following is a detailed introduction to the process of pairwise key establishment and authentication phase.

1) Pairwise Key Establishment Between Two Sensor Nodes: In our scheme, after the pairwise key established between two sensor nodes, nodes' predistribution keys are hashed. That is, if a node is predistributed a key $k_j^{(l,i)}$, after the pairwise key establishment phase, the node stores the following key: $Hk_j^{(l,i)} = H_{k_j^{(l,i)}}(\text{ID}_{a_l^i})$.

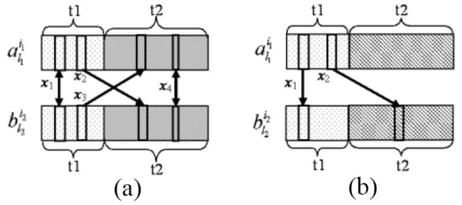


Fig. 4. Shared keys between two nodes when $l_1 = l_2$. In (a) $i_1 = i_2$, and in (b) $i_1 > i_2$.

Next, the process of pairwise establishment between two nodes $a_{l_1}^{i_1}$ $(a_{l_1}^{i_1} \in G_{l_1}^{i_1})$ and $b_l^{i_2}$ $(b_{l_2}^{i_2} \in G_{l_2}^{i_2})$ is described in detail.

If l_1 and l_2 are unequal and are not each other's neighbors, $a_{l_1}^{i_1}$ and $b_{l_2}^{i_2}$ cannot establish a pairwise key; otherwise, their common keys can be calculated according to the following cases.

1) If $l_1 = l_2$ and $i_1 = i_2$, as shown in Fig. 4(a), common keys of $a_{l_1}^{i_1}$ and $b_{l_2}^{i_2}$ consist of the following two parts.
   a) x_1 and x_4 common keys from $PLG_{l_2}^{i_2}$ and $PLC_{l_2}^{i_2}$, respectively.
   b) x_2 and x_3 common keys coming from $PLC_{l_2}^{i_2}$ and $PLC_{l_1}^{i_1}$, respectively.
2) If $l_1 = l_2$ and $i_1 > i_2$, $x_3 = x_4 = 0$, the value of x_1 and x_2 is same as the case 1 [see Fig. 4(b)].
3) If $l_1 \neq l_2$ and $i_1 = i_2$, $x_1 = x_4 = 0$, the value of x_2 and x_3 is same as the case 1.
4) If $l_1 \neq l_2$ and $i_1 > i_2$, $x_1 = x_3 = x_4 = 0$, the value of x_2 is same as the case 1.

If $x_1 + x_2 + x_3 + x_4 > 0$, the pairwise key between $a_{l_1}^{i_1}$ and $b_{l_2}^{i_2}$ is the XOR of all their common keys.

2) Authentication Between MS and Sensor Node:

Step 1: An MS broadcasts its predistribution keys' IDs.

Step 2: After sensor node a_l^i received these above keys' *IDs* from the MS, it seeks common keys with the MS from its key ring. a_l^i randomly selects SQ keys, namely $ck_1, \ldots, ck_{SQ}$, from the common key chains as authentication keys with the MS, and the formula for calculating SQ is as follows:

$$\text{SQ} = \text{BQ} + \text{DP} \times \text{AQ}, \text{ where SQ} \le T. \tag{4}$$

In formula (4), the formula for calculating DP is as follows:

$$DP = \begin{cases} DC_g - i, & DC_g - i < M_g \\ M_g, & DC_g - i \ge M_g. \end{cases} \tag{5}$$

Then a_l^i calculates the shared key $\text{SK}_{a_l^i-\text{MS}}$ with the MS: $\text{SK}_{a_l^i-\text{MS}} = ck_1 \oplus \cdots \oplus ck_{\text{SQ}}$, and generates a random number r, finally, it sends the following authentication information to the MS: $Au_{a_l^i-\text{MS}} = \{\text{ID}_{\text{MS}}, \text{ID}_{a_l^i}, r, \text{ID}_{ck_1}, \ldots, \text{ID}_{ck_{\text{SQ}}}, M_1\}$, where $M_1 = H_{\text{SK}_{a_l^i-\text{MS}}}(\text{ID}_{\text{MS}} \| \text{ID}_{a_l^i} \| r \| \text{ID}_{ck_1} \| \cdots \| \text{ID}_{ck_{\text{SQ}}})$.

Step 3: After received the above message, the MS calculates their shared key $\text{SK}_{\text{MS}-a_l^i}$ and authentication code: $M_1' = H_{\text{SK}_{\text{MS}-a_l^i}}(\text{ID}_{\text{MS}} \| \text{ID}_{a_l^i} \| r \| \text{ID}_{ck_1} \| \cdots \| \text{ID}_{ck_{SQ}})$. If $M_1 \neq M_1'$, then the authentication fails; otherwise, the MS sends the following message to $a_l^i : Au_{\text{MS}-a_l^i} = \{\text{ID}_{a_l^i}, \text{ID}_{\text{MS}}, M_2\}$, where $M_2 = H_{\text{SK}_{\text{MS}-a_l^i}}(\text{ID}_{a_l^i} \| \text{ID}_{\text{MS}} \| r + 1)$.

Step 4: After received the above message, a_l^i calculates $M_2' : M_2' = H_{\text{SK}_{a_l^i-\text{MS}}}(\text{ID}_{a_l^i} \| \text{ID}_{\text{MS}} \| r + 1)$. If and only if

$M_2 = M'_2$, a_l^i sends its data encrypted with the share key $\mathrm{SK}_{a_l^i-\mathrm{MS}}$ to the MS.

V. Performance and Security Evaluation

In this section, we analyze the performance and security of our scheme, including local connectivity, MS replication attack, and energy consumption.

In our analysis and simulations, we use the following setups.

1) The area is divided into hexagon cells and the length of a hexagon cell is 50, namely len = 50. The center of each cell is the deployment point (see Fig. 1). We assume that node deployment follows a 2-D Gaussian distribution.
2) The wireless communication range for a node is 40 m ($R = 40$ m).
3) We assume that an adversary randomly selects a cell and continuous to compromise nodes resides in the cell.
4) We assume that node deployment includes five phases. If the number of uncaptured nodes in a group is less than 30, then 60 nodes need to be added to it.
5) At each phase, the number of times that an MS collects data from the network is 120.
6) The size of the global key pool, namely m, is 70, and the length of the 3rd dimension of a 3-D backward key chain based on deployment knowledge is 50 ($L_3 = 50$).
7) The presented experimental data is an average of 50 replicates.

A. Local Connectivity Analysis

In our analysis, the connectivity includes the following two parts: 1) the probability of mutual authentication between an MS and a sensor node, namely PC_1 and 2) the probability of pairwise key establishment between two neighboring sensor nodes, namely PC_2.

1) Computing PC_1: In UWSNs, the predistribution keys of a sensor node and an MS is $t1 + t2$ and $t3$ ($t3 = m+T-t1-t2$), respectively. Obviously, the number of common 3-D backward key chains based on deployment knowledge between them is not less than T. Since the number of the common key chains that a sensor node needs to authenticate an MS does not exceed T, we can have that $\mathrm{PC}_1 = 1$.

2) Computing PC_2: In UWSNs, the construction process of local key pools shows that only two nodes from the same group or two neighbor groups can establish a shard key. Therefore, we can have the following formula for calculating PC_2:

$$\mathrm{PC}_2 = P_0 \cdot P_0^{\mathrm{SK}} + P_1 \cdot P_1^{\mathrm{SK}} \tag{6}$$

where P_0 and P_1 represent the probability of two nodes from the same group and two neighbor groups becoming neighbors, respectively, and P_0^{SK} and P_1^{SK} represent the probability of two nodes from the same group and two neighbor groups being able to establish a shared key, respectively.

The properties of the 2-D Gaussian distribution [29] indicate that P_0 and P_1 increase as σ decreases. From (6) it can be concluded that: as σ decreases, PC_2 increases. As shown in Fig. 5(a), when other parameters are constant, σ is reduced from 50 to 30, and the local connectivity in the first phase is increased from about 0.77 to 0.9. The key establishment process shows that the local connectivity is more susceptible to the parameter $t1$; the local connectivity decreases as the deployment phase increases. As shown in Fig. 5(b), when the value of $t1+t2$ is 40, $t1$ increases from 5 to 15, the local connectivity in the first phase increases from about 0.56 to 0.9; when the value of $t1$ is 10, from the first phase to the third phase, the local connectivity drops by about 0.16. However, it can be concluded from Fig. 5 that after the third phase, the local connectivity is basically stable. As shown in Fig. 5(b), $t1 = 10$, from the third phase to the fifth phase, the local connectivity drops by about 0.003.

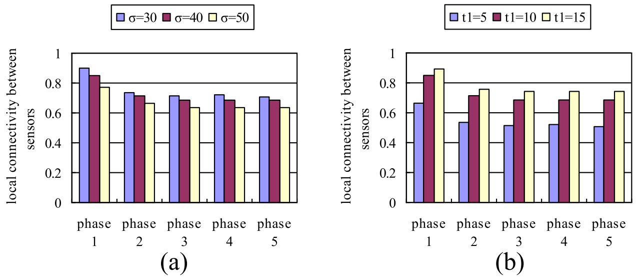


Fig. 5. Function of local connectivity between sensors and $t1$, $t2$, and σ. (a) $t1 = 10$ and $t2 = 30$. (b) $\sigma = 40$ and $t1 + t2 = 40$.

B. Resilience Against Mobile Sink Replication Attack

In this paper, after Ith phase capture (for the convenience of description, in the following formulas, superscript I represents the Ith capture), resilience against MS replication attack, namely Pr^I can be evaluated by the ratio of the number of uncaptured nodes which can successfully authenticate a replication MS to the total number of uncaptured nodes. And Pr^I can be estimated as follows:

$$\mathrm{Pr}^I = \frac{\sum_{l\in[1,L]} \sum_{i=1}^{I} SN_l^{I,i} \cdot \mathrm{Pr}_l^{I,i}}{\sum_{l\in[1,L]} SN_l} \tag{7}$$

where $SN_l^{I,i}$ represents the set of uncaptured nodes whose deployment points locate in the cell l and whose deployment phase is i (for the convenience of description, in the following formulas, superscript i means nodes of the ith phase or keys of the ith generation of a local key pool). $\mathrm{Pr}_l^{I,i}$ is the probability that nodes in the set $SN_l^{I,i}$ and the replication MS can authenticate each other. Let $m_l^{I,i}$ is the expected value of the number of compromised key chains in the local key pool PL_l^i. The calculation of $\mathrm{Pr}_l^{I,i}$ should be considered in the following three cases.

1) When $m_l^{I,i} < \mathrm{SQ}$, $\mathrm{Pr}_l^{I,i} = 0$.
2) When $m_l^{I,i} = m$, $\mathrm{Pr}_l^{I,i} = 1$.
3) When $\mathrm{SQ} \leq m_l^{I,i} < m$, the calculation process of $\mathrm{Pr}_l^{I,i}$ is analyzed as follows.

The number of ways for selecting x ($T \leq x \leq t1 + t2$) common keys shared between a sensor node and an MS is

$$\sum_{x=T}^{t1+t2} \binom{m}{x} \cdot \binom{m-x}{t1+t2+t3-2x} \cdot \binom{t1+t2+t3-2x}{t1+t2-x}.$$

It is assumed that $x1$ and $x2$ represent the number of keys from the captured key pool and the uncaptured key pool, respectively, which are shared between an MS and a sensor node. The number of ways for selecting these keys is

$$\binom{m_l^{I,i}}{x_1}\cdot\binom{m-m_l^{I,i}}{x_2}\cdot\binom{m-m_l^{I,i}-x_2}{t1+t2+t3-2x_1-2x_2}\cdot\binom{t1+t2+t3-2x_1-2x_2}{t3-x_1-x_2}.$$

If and only if a sensor node selects SQ keys from $x1$ as authentication keys with a replication MS, then the replication MS can be authenticated by the sensor node. Therefore, if the sensor node and the MS have $x1 + x2$ common keys, the probability that the replication MS can be authenticated by the sensor node is: $[\binom{x_1}{SQ}/\binom{x_1+x_2}{\mathrm{SQ}}]$.

In summary, $\mathrm{Pr}_l^{I,i}$ can be estimated by the following formula:

$$\underset{l}{\overset{I,i}{\mathrm{Pr}}}=\begin{cases}0, \quad \text{when } m_l^{I,i}<\mathrm{SQ}\\ \dfrac{\sum_{x_1=\mathrm{SQ}}^{S_1}\binom{m_l^{I,i}}{x_1}\cdot\sum_{x_2=S_2}^{S_3}\dfrac{\dfrac{\binom{m-m_l^{I,i}}{x_2}\cdot\binom{m-m_l^{I,i}-x_2}{t1+t2+t3-2x_1-2x_2}}{\left(\mathrm{SQ}^{x_1+x_2}\right)}}{\binom{t1+t2+t3-2x_1-2x_2}{t3-x_1-x_2}\cdot\left(\mathrm{SQ}^{x_1}\right)}}{\sum_{x=T}^{t1+t2}\binom{m}{x}\cdot\binom{m-x}{t1+t2+t3-2x}\cdot\binom{t1+t2+t3-2x}{t1+t2-x}}\\ \text{when } \mathrm{SQ}\le m_l^{I,i}<m\\ 1, \quad \text{when } m_l^{I,i}=m\end{cases} \tag{8}$$

where $S_1 = \min(t1 + t2, m_l^{I,i})$, $S_2 = \max(T + m_l^{I,i} - x_1, 0)$, and $S_3 = \min(t1 + t2 - x1, m - m_l^{I,i})$, $m_l^{I,i}$ can be estimated by the following formula:

$$m_l^{I,i}{=}m\times\left(1-\mathrm{PLGr}_l^{I,i}\cdot\mathrm{PLCr}_l^{I,i}\right) \tag{9}$$

where $\mathrm{PLGr}_l^{I,i}$ and $\mathrm{PLCr}_l^{I,i}$ represent the probability that keys in PLG_l^i and PLC_l^i are not compromised, respectively.

1) Computing $PLGr_l^{I,i}$: In our scheme, the method for constructing the key pool PG shows: it is not feasible in calculation to get keys in PG by using keys from an ordinary key pool. And the shared key establishment process shows that if sensor node a_l^i completes the establishment of the shared key with its neighbor nodes, then an adversary cannot obtain any keys information of PLG_l^i by compromising a_l^i; otherwise if sensor node a_l^i is captured, it only can reveal $t1$ keys of $\mathrm{PLG}_l^{i_1}$ ($i_1 \leq i$). Therefore, the probability that keys in PLG_l^i are not compromised, namely $\mathrm{PLGr}_l^{I,i}$, can be calculated as follows:

$$\mathrm{PLGr}_l^{I,i}=\left(1-\frac{t1}{m}\right)^{\sum_{i_2=i}^{I}CC_l^{i_1}} \tag{10}$$

where $CC_l^{i_1}$ represents the number of nodes from the group $G_l^{i_1}$, which are compromised in the shared key establishment phase.

2) Computing $PLCr_l^{I,i}$: In our scheme, $k_j^{(s_l,i_1,l')}$ can be calculated by using $k_j^{(s_l,i)}$ ($i_1 \leq i$, $1 \leq l' \leq L$). In addition, there are seven parts of keys in LG_l^i, and six parts of them are, respectively, assigned to the six neighbors of the cell l. So, neighbor nodes of the cell l captured in the key establishment phase can also expose the key information of PLC_l^i. When $a_{l'}^i$ ($l' \in \{l\} \cup NC_l$, where NC_l is the set of the cell l's neighboring cells) is compromised, the probability of keys in PLC_l^i, not being compromised because of $t1$ and $t2$ keys being predistributed to it is $([\sum_{l'\in\{l\}\cup NC_l}(1-[t1/m])^{\sum_{i_2=i}^{I}CC_{l'}^{i_1}}]/7)$ and $(1-([t2]/[m\cdot L']))^{CC_l^i}$, respectively. As a result, the probability of keys in PLC_l^i not being compromised, namely $\mathrm{PLCr}_l^{I,i}$, can be estimated as follows:

$$\mathrm{PLCr}_l^{I,i}=\left(1-\frac{t2}{m\cdot L'}\right)^{CC_l^i}\cdot\frac{\sum_{l'\in\{l\}\cup NC_l}\left(1-\frac{t1}{m}\right)^{\sum_{i_2=i}^{I}CC_{l'}^{i_1}}}{7}. \tag{11}$$

It can be concluded from (7) and (8) when other parameters are constant, Pr^I decreases as T increases. As shown in Fig. 6(a), when T increases from 25 to 35, Pr^5 is reduced from about 0.07 to 0.007. It can be seen from (4) and (5) when $\mathrm{Mg} = 0$ or $\mathrm{AQ} = 0$, $\mathrm{SQ} = \mathrm{BQ}$, and this scheme degenerates into the q scheme. Equation (8) indicates that $\mathrm{Pr}_l^{I,i}$ increases as I-i increases, eventually resulting in an increase in Pr^I. As shown in Fig. 6(b) and (d), when $\mathrm{Mg} = 0$ or $\mathrm{AQ} = 0$, Pr^1 and Pr^5 is about 0.002 and 0.03, respectively. Pr^I decreases as BQ, AQ, and Mg increase. However, the magnitude of the decrease becomes smaller as BQ, AQ, and Mg increase. As shown in Fig. 6(e), when Mg increases from 0 to 2 and increases from 2 to 4, Pr^5 decreases by 0.009 and 0.002, respectively; when BQ increases from 5 to 7 and increases from 7 to 9, Pr^5 decreases by 0.009 and 0.003, respectively; and when AQ increases from 0 to 2 and increases from 2 to 4, Pr^5 decreases by 0.01 and 0.007, respectively. Equations (10) and (11) show that $\mathrm{Pr}_l^{I,i}$ increases significantly as the number of sensor nodes captured during the shared key establishment phase increases. This can be confirmed from Fig. 6(f). For example, during each deployment phase, if the number of nodes captured during the pairwise key established between two sensor nodes is CC, when it increases from 10 to 20, Pr^5 increases from about 0.001 to 0.023.

C. Energy Consumption

In this paper, we adopted the energy model proposed in [32]. The amount of energy needed by the radio to transmit an l-bit message a distance d is given as

$$\mathrm{ET}(l,R)=\mathrm{ET}_{\mathrm{elec}}(l)+\mathrm{ET}_{\mathrm{amp}}(l,R)=l\cdot E_{\mathrm{elec}}+l\cdot\varepsilon\cdot R^2 \tag{12}$$

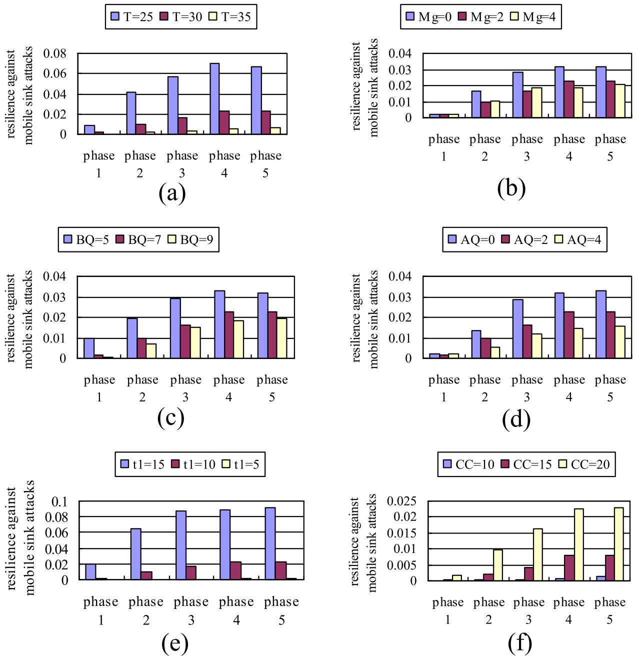
where $\mathrm{ET}_{\mathrm{elec}}(l)$ represents the electronics energy and $\mathrm{ET}_{\mathrm{amp}}(l,R)$ is the amplifier energy. R represents the maximum distance between the transmitter and the receiver. The communication energy parameters are set as

$$E_{\mathrm{elec}}=50\ \mathrm{nJ/bit},\ \ \varepsilon=10\ \mathrm{pJ/bit/m^2}.$$

To receive a message, the radio expends

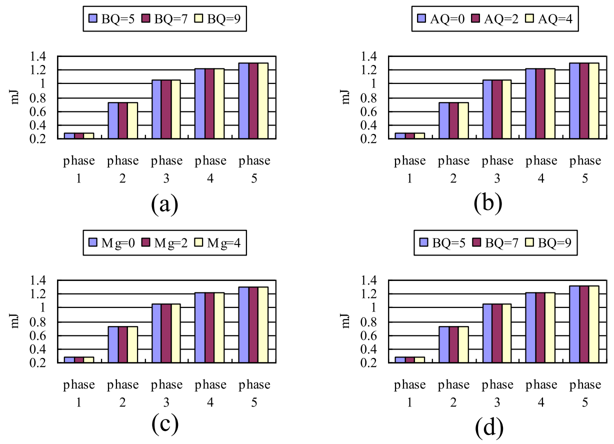
$$\mathrm{ER}(l,R)=\mathrm{ET}_{\mathrm{elec}}(l)=l\cdot E_{\mathrm{elec}}. \tag{13}$$

Fig. 7 shows that the effect of different parameters on the average energy consumption of a sensor node. In our simulations, nodes' ID is 2 bytes, keys' ID is 3 bytes, the authentication code is 4 bytes, and a random number and a key are 8 bytes. And in our scheme, we can know from the key



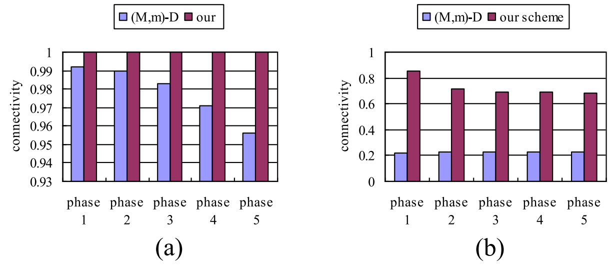
(a) (b) (c) (d) (e) (f)

Fig. 6. Function of resilience against MS replication attack and *T*, *BQ*, *AQ*, *t*1, *Mg*, and *CC*. (a) BQ = 7, AQ = 2, t1 = 30, t2 = 10, Mg = 2, and CC = 20. (b) T = 30, BQ = 7, AQ = 2, t1 = 10, t2 = 30, and CC = 20. (c) T = 30, AQ = 2, t1 = 30, t2 = 10, Mg = 2, and CC = 20. (d) T = 30, BQ = 7, t1 = 30, t2 = 10, and Mg = 2. (e) T = 30, BQ = 7, AQ = 2, $t1 + t2 = 40$, Mg = 2, and CC = 20. (f) T = 30, BQ = 7, AQ = 2, t1 = 10, t2 = 30, and Mg = 2.



(a) (b) (c) (d)

Fig. 7. Function of energy consumption and *T*, *BQ*, *AQ*, and *Mg*. In the figure, $t1 + t2 = 40$. In (b)–(d), *T* = 30. (a) AQ = 2, Mg = 2, and T = 30. (b) BQ = 7, Mg = 2, and T = 30. (c) BQ = 7, Mg = 2, and T = 30. (d) AQ = 2, Mg = 2, and T = 35.



(a) (b)

Fig. 8. Comparing connectivity results. (a) Between a mobile sink and an sensor node. (b) Between two sensor nodes.

establishment and authentication process that the amount of information sent by a node will increase with the increase of *BQ*, *AQ*, and *Mg*. However, the amount of information added is small, and the increased energy consumption is almost negligible (see Fig. 7). The amount of information received by a node increases as *T* and the number of neighbor nodes increase. However, the amount of information added because of the increase of *T* is small, and the increased energy consumption is almost negligible (see Fig. 7). In our scheme, there are two reasons for the significant increase in energy consumption after the first phase.

1) When a group has fewer than 30 nodes, 60 nodes are needed to be deployed to the area. This leads to an increase in the number of nodes' neighbors. Since a node needs to receive the IDs of the predistribution key chains of each neighbor node during the shared key establishment phase. This resulting in a significant increase in the amount of information received.
2) If nodes deployed in the *i*th phase are not captured in the subsequent *j* phases, then they are needed to receive the IDs of the predistribution key chains of their neighbor nodes multiple times during the shared key establishment phase. This resulting in an increase in the amount of information received.

As shown in Fig. 7, when $T = 35$, BQ = 9, AQ = 2, and Mg = 2, compared with the previous phase, the energy consumption increments of the second phase to the fifth phase are about 0.44, 0.33, 0.17, and 0.09 mJ, respectively.

D. Comparison With the Existing Schemes

In this section, performance of our scheme and (*M*, *m*) scheme is compared [11]. For the sake of fairness, (*M*, *m*) scheme is merged with a scheme based on deployment knowledge. The modified (*M*, *m*) scheme is called as (*M*, *m*)-D scheme. In (*M*, *m*)-D, the division of target area, the models of node deployment and capture, are same as our scheme. And in (*M*, *m*)-D, each group uses a separate key pool, which consists of 2-D symmetric key polynomials [15] with a degree of 100. The size of each key pool is 14, an MS is predistributed 13 shared parts of 2-D symmetric polynomials from each key pool, and each node is predistributed the shared portion of three 2-D symmetric polynomials from its own group key pool. In our simulations, *M* and *m* are 30 and 3, respectively, and a node randomly selects 25 nodes from *M* to participate in the authentication between an MS and a sensor node. And assume that 80% of the captured sensor nodes are identified as capture nodes by normal nodes [30], [31].

Fig. 8 shows the comparison results of the local connectivity. Fig. 8(a) and (b) shows the probability comparison that an MS and a sensor can authenticate each other (PC_1) and the probability comparison that two neighboring sensor nodes can establish a shared key (PC_2).

From the previous analysis, in our scheme, PC_1 is 1 at any time. However, in (*M*, *m*)-D, a sensor node wants to establish a shared key with an MS, which requires at least

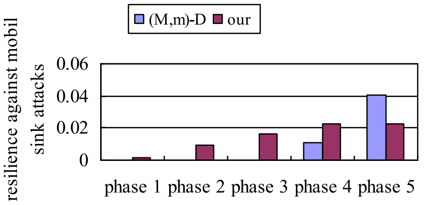


Fig. 9. Comparing resilience against MS replication attack results.

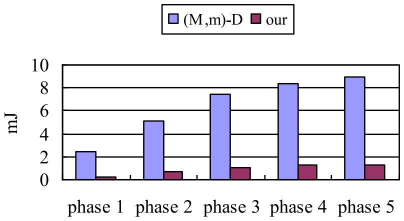


Fig. 10. Comparing energy consumption.

m neighbors to provide the correct joint authentication messages. If captured neighbor nodes do not provide the correct joint authentication messages and when there are many nodes captured, the MS cannot establish a correct shared key with the sensor node because it does not get enough correct joint authentication messages. In the (M, m)-D scheme, this attack is called as DoS attack. Obviously, PC_1 decreases as the probability of successfully initiating DoS attack increases. As shown in Fig. 8(a), PC_1 in the first phase and the fifth phase is about 0.992 and 0.952, respectively.

From the previous analysis, in our scheme, we can see that PC_2 tends to be stable after the third phase. From Fig. 8(b), it can be concluded that although PC_2 of (M, m)-D scheme remains stable at each phase, its value is much less than our scheme. For example, in the fifth phase, PC_2 of our scheme and (M, m)-D scheme is about 0.68 and 0.23, respectively. In (M, m)-D scheme, the local connectivity can be increased by increasing the number of symmetric polynomials predistributed to a sensor node. However, the captured nodes will leak more key information, which is more disadvantageous against DoS attack and MS replication attack.

Fig. 9 shows a comparison of Pr^I, that is, resilience of replication attack in each phase. In (M, m)-D scheme, if an adversary can be authenticated by sensor nodes, then he can successfully initiate a replication attack. In our simulations, if an MS shares three 2-D symmetric key polynomials with a sensor node, then it can be authenticated by the sensor node. That is, when the compromised 2-D symmetric key polynomials are less than 3, the adversary cannot successfully initiate an MS replication attack. As shown in Fig. 9, Pr^I ($I \leq 3$) is 0. However, when the compromised 2-D symmetric key polynomial is not less than 3, the adversary can successfully initiate an MS replication attack by jointing the compromised neighbor nodes which are not correctly identified. In (M, m)-D scheme, key pools of each phase remain unchanged, Pr^I rises faster. In our scheme, 3-D backward key chains based on deployment knowledge is used, key pool of each phase is independent, and Pr^I rises slowly. As shown in Fig. 9, in (M, m)-D and our scheme, Pr^5 is about 0.04 and 0.022, respectively.

Fig. 10 shows a comparison of the energy consumption required to establish a shared key in each phase. In (M, m)-D scheme, the probability of directly establishing a shared key between two sensor nodes is not high, to improve the resilience of DoS attack and MS replication attack, M neighbor nodes participating in joint authentication are required to provide key information. In our simulations, M is 30, and the average number of neighbor nodes is about 50. The analysis of the local connectivity shows that the number of nodes those can be directly selected as joint authentication is about $50 \times 0.23 \approx 12$, which is much smaller than 30. Therefore, the path key establishment process must be initiated to establish a shared key for two neighboring nodes those cannot directly establish a shared key. The path key establishment is generally carried out in a flooding manner, and the energy consumption is large. In our scheme, there is no path key establishment process because the local connectivity is high and no neighbor nodes need to be involved in the process of authentication between an MS and a sensor node. Therefore, in our scheme, the energy consumption of each phase is much lower than the (M, m)-D scheme. For example, in the fifth phase, the energy consumption of our scheme and (M, m)-D scheme is about 1.3 and 8.9 mJ, respectively. In addition, the analysis of Section V-C shows that the energy consumption of nodes increases with deployment phase increases. This conclusion can be confirmed from Fig. 10.

VI. Conclusion

In this paper, based on deployment knowledge, we propose an efficient anti-replication MS attack scheme. First, we construct 3-D backward key chains based on deployment knowledge. Then we propose an authentication method for anti-replication MS attack. Analysis and simulation show the following.

1) Authentication between an MS and a sensor node is enhanced, and the ability to resist MS replication attack is improved. For example, when $T = 30$, $\mathrm{BQ} = 7$, $\mathrm{AQ} = 2$, $\mathrm{Mg} = 2$, $t1 = 10$, $t2 = 30$, and $CC = 20$, in the fifth phase, the probability that an adversary can successfully initiate an MS replication attack is about 0.022.
2) Due to the use of 3-D backward key chains based on deployment knowledge, the information received by a node does not change with the increase of the deployment area, and its energy consumption is significantly reduced. In our simulations, the energy consumption does not exceed 1.4 mJ.
3) The proposed scheme not only ensures that a sensor node and an MS can directly authenticate each other, but also enables a high probability of establishing a shared key between two sensor nodes. For example, in the fifth phase, if the standard deviation σ of the 2-D Gaussian distribution is 40, $m = 70$, $t1 = 10$, and $t2 = 30$, the local connectivity is about 0.68.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] D. Ma, C. Soriente, and G. Tsudik, "New adversary and new threats: Security in unattended sensor networks," *IEEE Netw.*, vol. 23, no. 2, pp. 43–48, Mar. 2009.

[3] R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Catch me (if you can): Data survival in unattended sensor networks," in *Proc. IEEE PERCOM*, Hong Kong, 2008, pp. 185–194.

[4] R. Di Pietro, G. Oligeri, C. Soriente, and G. Tsudik, "United we stand: Intrusion resilience in mobile unattended WSNs," *IEEE Trans. Mobile Comput.*, vol. 12, no. 7, pp. 1456–1468, Jul. 2013.

[5] R. Di Pietro and N. V. Verde, "Epidemic data survivability in unattended wireless sensor networks," in *Proc. ACM WiSec*, Hamburg, Germany, 2011, pp. 11–22.

[6] Y. Ren, V. A. Oleshchuk, and F. Y. Li, "Optimized secure and reliable distributed data storage scheme and performance evaluation in unattended WSNs," *Comput. Commun.*, vol. 36, no. 9, pp. 1067–1077, May 2013.

[7] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, "A novel approach to trust management in unattended wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 7, pp. 1409–1423, Jul. 2014.

[8] A. Rasheed and R. N. Mahapatra, "Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks," *IEEE Trans. Parallel Distrib. Syst*, vol. 22, no. 1, pp. 176–184, Jan. 2011.

[9] S. Li, W. Wang, B. Zhou, J. Wang, Y. Cheng, and J. Wu, "A secure scheme for heterogeneous sensor networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 182–185, Apr. 2017.

[10] A. Rasheed and R. N. Mahapatra, "The three-tier security scheme in wireless sensor networks with mobile sinks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 5, pp. 958–965, May 2012.

[11] S. Li, W. Wang, B. Zhou, J. Wang, Y. Cheng, and J. Wu, "A (M, m) authentication scheme against mobile sink replication attack in unattended sensor networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 2, pp. 250–253, Apr. 2018.

[12] K. Piotrowski P. Langendoerfer, and S. Peter, "How public key cryptography influences wireless sensor node lifetime," in *Proc. ACM SASN*, 2006, pp. 169–176.

[13] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM CCS*, 2002, pp. 41–47.

[14] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Security Privacy*, 2003, pp. 197–213.

[15] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly secure key distribution for dynamic conferences," in *Proc. CRYPTO*, 1992, pp. 471–486.

[16] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," *IEEE Trans. Depend. Secure Comput.*, vol. 3, no. 1, pp. 62–77, Jan./Mar. 2006.

[17] Z. Yu and Y. Guan, "A key management scheme using deployment knowledge for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 10, pp. 1411–1425, Oct. 2008.

[18] A. Fanian, M. Berenjkoub, H. Saidi, and T. A. Gulliver, "A high performance and intrinsically secure key establishment protocol for wireless sensor networks," *Comput. Netw.*, vol. 55, no. 8, pp. 1849–1863, 2011.

[19] B. Zhou, S. Li, Q. Li, X. Sun, and X. Wang, "An efficient and scalable pairwise key pre-distribution scheme for sensor networks using deployment knowledge," *Comput. Commun.*, vol. 32, no. 1, pp. 124–133, 2009.

[20] B. Zhou, J. Wang, S. Li, and W. Wang, "A new key predistribution scheme for multiphase sensor networks using a new deployment mode," *J. Sensors*, vol. 2014, p. 10, May 2014.

[21] B. Zhou, J. Wang, S. Li, W. Wang, Y. Cheng, and J. Wu, "A secure scheme based on layer model in multi-phase sensor networks," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1421–1424, Jul. 2016.

[22] K. Ren, K. Zeng, and W. Lou, "A new approach for random key predistribution in large-scale wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 6, no. 3, pp. 307–318, 2006.

[23] W. Bechkit, Y. Challal, and A. Bouabdallah, "A new class of hashchain based key pre-distribution schemes for WSN," *Comput. Commun.*, vol. 36, no. 3, pp. 243–255, 2013.

[24] S. Li, B. Zhou, J. Dai, and X. Sun, "A secure scheme of continuity based on two-dimensional backward hash key chains for sensor networks," *IEEE Wireless Commun. Lett.*, vol. 1, no. 5, pp. 416–419, Oct. 2012.

[25] B. Zhou, S. Li, J. Wang, S. Yang, and J. Dai, "A pairwise key establishment scheme for multiple deployment sensor networks," *Int. J. Netw. Security*, vol. 16, no. 3, pp. 229–236, 2014.

[26] B. Zhou, J. Wang, S. Li, Y. Cheng, and J. Wu, "A continuous secure scheme in static heterogeneous sensor networks," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1868–1871, Sep. 2013.

[27] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," in *Proc. 10th ACM Conf. Comput. Commun. Security (CCS)*, Oct. 2003, pp. 52–61.

[28] S. Hussain, F. Kausar, and A. Masood, "An efficient key distribution scheme for heterogeneous sensor networks," in *Proc. Int. Conf. Wireless Commun. Mobile Comput. (IWCMC)*, 2007, pp. 388–392.

[29] A. Leon-Garcia, *Probability and Random Processes for Electrical Engineering*, 2nd ed. Reading, MA, USA: Addison-Wesley, 1994.

[30] X. Du, "Detection of compromised sensor nodes in heterogeneous sensor networks," in *Proc. ICC*, Beijing, China, 2008, pp. 1446–1450.

[31] Q. Zhang, T. Yu, and P. Ning, "A framework for identifying compromised nodes in wireless sensor networks," *ACM Trans. Inf. Syst. Security*, vol. 11, no. 3, pp. 1–37, 2008.

[32] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, Oct. 2002.

Boqing Zhou received the Ph.D. degree in computer science from Hunan University, Changsha, China, in 2011.

He is currently a Vice Professor with the School of Information Science and Engineering, Shaoguan University, Shaoguan, China. His current research interests include sensor networks and information security.

Sujun Li received the Ph.D. degree in computer science from Central South University, Changsha, China, in 2018.

She is currently a Vice Professor with the School of Information Science and Engineering, Shaoguan University, Shaoguan, China. Her current research interests include sensor networks and information security.

Weiping Wang (M'13) received the Ph.D. degree in computer science from Central South University, Changsha, China, in 2004.

She is currently a Professor with the Department of Information Science and Engineering, Central South University. Her current research interests include network optimization, network encoding, network security, and anonymous communication.

Jianxin Wang (SM'12) received the Ph.D. degree in computer science from Central South University, Changsha, China, in 2006.

He is currently a Professor with the Department of Information Science and Engineering, Central South University. He has published over 100 papers in various international journals and refereed conferences. His current research interests include algorithm analysis and optimization, computer network, and bioinformatics.

Yun Cheng received the Ph.D. degree in computer science from the National University of Defense Technology, Changsha, China, in 2001.

He is currently a Professor with the School of Hunan Institute of Humanities, Science and Technology, Loudi, China. His current research interests include algorithm analysis and computer network.

Jie Wu (F'09) received the B.S. degree in computer engineering and the M.S. degree in computer science from the Shanghai University of Science and Technology, Shanghai, China, in 1982 and 1985, respectively, and the Ph.D. degree in computer engineering from Florida Atlantic University, Boca Raton, FL, USA, in 1989.

He is the Chair and a Laura H. Carnell Professor with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA, USA. He was a Program Director with the National Science Foundation, Alexandria, VA, USA, and a Distinguished Professor with Florida Atlantic University, Boca Raton, FL, USA. He regularly publishes in scholarly journals, conference proceedings, and books. His current research interests include mobile computing and wireless networks, routing protocols, cloud and green computing, network trust and security, and social network applications.

Dr. Wu was a recipient of the 2011 China Computer Federation (CCF) Overseas Outstanding Achievement Award. He serves on several editorial boards, including the IEEE TRANSACTIONS ON SERVICE COMPUTING and the *Journal of Parallel and Distributed Computing*. He was the General Co-Chair/Chair of the IEEE MASS 2006, the IEEE IPDPS 2008, the IEEE ICDCS 2013, and ACM MobiHoc 2014, as well as the Program Co-Chair of the IEEE INFOCOM 2011 and CCF CNCC 2013. He was an IEEE Computer Society Distinguished Visitor, an ACM Distinguished Speaker, and the Chair of the IEEE Technical Committee on Distributed Processing. He is a CCF Distinguished Speaker.