This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2770119, IEEE Wireless Communications Letters

A (*M*,*m*) Authentication Scheme against mobile sink replicated Attack in Unattended Sensor Networks

Sujun Li, Weiping Wang, Boqing Zhou, Jianxin Wang, Yun Cheng, Jie Wu, IEEE Fellow

***Abstract*—In some non-real time applications, data is collected by Mobile Sinks. This kind of networks is vulnerable to Mobile Sinks (MS) replicated attack. In this attack, replicated MSs can collect data from sensor nodes by establishing pairwise keys with them using keys information obtained from captured sensors. In this paper, a (*M*,*m*) authentication scheme against the attack is proposed. The analysis and simulation results indicate that the scheme can improve networks' resilience against MS replicated attack as compared with existing schemes.**

***Index Terms*—unattended Sensor networks, MS replicated attack, security communication protocol.**

I. Introduction

In non-real time applications, the size of the surveillance area would require an MS to collect data periodically [1-2]. We refer to such networks as unattended sensor networks (USNs) [1-2]. USNs are vulnerable to MS replicated attack [2]. In this attack, replicated MSs can collect data from sensor nodes by establishing pairwise keys with them based on keys information obtained from captured sensors.

To improve the resilience against replicated attack, authentication and pairwise key establishment between sensor nodes and MSs, are important. In sensor networks, some key establishment schemes have been proposed [2-6]. EG scheme was the first key pre-distribution scheme [3], in which each sensor picks some keys randomly from a large key pool before deployment. Two sensors can establish a shared key, if they share at least one common key. To enhance the security of the EG scheme against small-scale attacks, *q*-composite scheme was proposed [4], in which *q* common keys are required for two nodes to establish a shared key. To improve the network resilience against node capture, an enhanced scheme using bivariate t-degree polynomials [5] was proposed [6]. In mobile networks, if the above schemes are used directly for authentication and pairwise key establishment between sensor nodes and MSs, then it is vulnerable to MS replicated attack. On the basis of schemes in [4, 6, 7], a three-layer communication model was proposed [2], namely ETTS, which can improve resilience against MS replicated attack. In ETTS, authentication between MSs and static access nodes and between static access nodes and sensor nodes is achieved with a certain probability. Although the scheme's resilience against MS replicated attack is improved, attackers can collect data from network by using replicated static access nodes. Recently, Li et al proposed an EQ scheme can significantly improve resilience against powerful sensors (e.g., PDAs) attack in heterogeneous sensor networks [8]. In USNs, if EQ scheme is directly used, the probability of establishing shared key between sensor nodes and MSs is low. Therefore, in mobile networks, to improve networks' resilience against MS replicated attack, new authentication mechanism is needed to be developed.

In this paper, a (*M*,*m*) authentication scheme against MS replicated attack is proposed for USNs. Main contributions of our scheme are summarized as follows: 1. A (*M*,*m*) model is proposed. In this model, an MS can collect data from a sensor if and only if it can establish shared key with the sensor and it can pass through authentication of at least *m* neighbors chosen from *M* neighbors of the sensor. 2. Analysis and simulation results show that our scheme can significantly improve networks' resilience against MS replicated attack as compared with existing schemes.

The paper is organized as follows. Section II presents our scheme Section III analyzes the scheme. Section IV concludes the paper.

This work is partially supported by the HPCSIP Key Laboratory, Ministry of Education, the Research Foundation of Education Committee of Hunan Province, China under grant no. 16A110 and 12C0742, the National Natural Science Foundation of China under grant no. 61672543.

S. Li is with the School of Information Science and Engineering, Central South University, Changsha 410083, China (e-mail: sujunli@mail.csu.edu.cn), and also with the Department of Information, Hunan University of Humanities, Science and Technology, Loudi 417000, China.

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).

B. Zhou and Y. Cheng is with the Department of Information, Hunan University of Humanities, Science and Technology, Loudi 417000, China (e-mail: zbq_paper@163.com; 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).

Corresponding Authors: W. wang (e-mail: wpwang@mail.csu.edu.cn), B. Zhou (zbq_paper@163.com).

II. Our Scheme

A. Notation and assumption

For the convenience of description, we use the following notations:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2770119, IEEE Wireless Communications Letters

Table I notations

DN	The number of nodes deployed
CN	The number of nodes captured
CC	The number of nodes captured during the key establishment and delivery stage
Ar	The size of deployment area
ID_{fi}	The ID of the polynomial $f_i(x,y)$
ID_{MS}	The ID of MS
$K_{a\text{-}b}$	The shared key established between nodes *a* and *b*
Au_a	The neighbor authentication set of node *a*. Any a node in the set shares no less than *q* keys with an MS
$E_k(inf)$	The information *inf* is encrypted by symmetric encryption algorithm *E* with the key *K*
$H_k(inf)$	The MAC of the message *inf*, which is generated by Hash *H* with the key *k*
$inf_1 \mid inf_2$	concatenating the message *inf1* and *inf2*
$inf_1 \oplus inf_2$	XOR the information *inf1* and *inf2*
|S|	The size of set *S*

In the scheme, we suppose that if an attacker captures a sensor, all key information it holds will also be compromised. Moreover, the 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 replicated attack [2], DoS attack, etc. At the same time, we suppose that only a limited number of nodes may be compromised by an attacker during the short time period of key establishment and delivery stage [9].

B. Key pre-distribution stage

In our scheme, shared key between two nodes is generated by bivariate t-degree polynomials [5]. And the polynomial $f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^i y^j$ is generated in the finite field F_q, where *q* is a prime number that is large enough to accommodate a cryptographic key, and it meets $f(x,y)=f(y,x)$. It is assumed that each sensor node has a unique ID. For a node with ID *a*, a polynomial share, namely $f(a,y)$, is pre-distributed to it. Thus, for any two sensor nodes with ID *a* and *b*, they can calculate their shared key $f(a,b)$ by exchanging their IDs.

They key pool consists of *n* bivariate t-degree polynomials and their *IDs*. An MS and a sensor node randomly picks $t1$ and $t2$ ($t2<<t1$) polynomials from the key pool, respectively. $f_l(x,y)$ denotes the l^{th} pre-distribution polynomial. Each node calculates and stores the shared parts of these polynomials.

C. Authentication model

In our scheme, a sensor node sends its data to an MS only when the MS passes through the sensor node's authentication. Our authentication model consists of key establishment and delivery, and authentication between sensor nodes and MSs two stages.

1) Key establishment and delivery stage

Step 1.After deployment, each node broadcasts its ID and its polynomials' ID. If two neighbor nodes *a* and *b* share *L* ($L\geq1$) polynomials $f_1(x,y)$, …, $f_L(x,y)$, then *a* and *b* calculate their shared key $K_{a-b}=f_1(a,b)\oplus\cdots\oplus f_L(a,b)$. Otherwise, a key path will be formed between them. On the key path, two neighbor nodes share common keys. Then, any one of the two nodes randomly generates a key *K* and securely sends it to another node along the key path.

Step 2. Node *a* randomly chooses *M* neighbors to form its candidate authentication set CA_a, and stores their polynomials' IDs. Then, *a* sends authentication key information request to these nodes. When node *b* receives the above request message, it selects polynomials which are from its pre-distribution polynomials and are not shared with *a*, namely $f_1(b,y)$, …, $f_{L1}(b,y)$. At last, node *b* calculates the values $f_1(b,a)$, …, $f_{L1}(b,a)$, and sends the message $U_{b-a}=\{a,b,E_{k_{b-a}}(inf),M_{b-a}\}$ (where $inf=\{f_1(b,a),\cdots,f_{L_1}(b,a)\}$, $M_{b-a}=H_{K_{b-a}}(a\,|\,b\,|\,inf)$) to *a*.

Step 3. When *a* receives $U_{b\text{-}a}$, it decrypts $U_{b\text{-}a}$ with $K_{a\text{-}b}$ getting *inf*. Then it recalculates message authentication code $M_{a\text{-}b}$. If $M_{a\text{-}b}=M_{b\text{-}a}$, *a* stores *inf*.

2) Authentication between MSs and sensor nodes

Step 1. An MS broadcasts its ID and its polynomials' IDs. In this paper, it is supposed that MSs and sensor nodes have the same transmission radius.

Step 2. When node *a* receives the above message, it calculates the value of all polynomials shared with the MS, $f_1(a,ID_{MS})$, …, $f_{L2}(a,ID_{MS})$. If $L_2\geq q$, *a* determines the authentication set Au_a from CA_a. If $|Au_a|\geq m$, *a* sends a message $inf_{a\text{-}MS}=\{ID_a,k_r,|Au_a|,ID_{f_1},\cdots,ID_{f_{L_2}}\}$ (where k_r is the random number generated by *a*) to the MS. Otherwise, authentication between *a* and the MS fails.

Step 3. When the MS receives $inf_{a\text{-}MS}$, it calculates their shared key $K_{MS\text{-}a}$. And sends a message $inf_{MS\text{-}a}=\{a,MAC_{MS-a}\}$ ($MAC_{MS-a}=H_{K_{MS-a}}(k_r+1)$) to *a*.

Step 4. When *a* receives $inf_{MS\text{-}a}$, it calculates their shared key $K_{a\text{-}MS}$ and recalculates MAC_{a-MS}. If $MAC_{a-MS}\neq MAC_{MS-a}$, authentication fails; Otherwise, *a* sends authentication request message $RA_a=\{ID_a,inf_{MS}\}$ to its neighbors. When *b* receives RA_a, and finds the polynomials, namely $f_1(b,y)$, …, $f_{L3}(b,y)$, shared with the MS. If $L_3\geq q$, *b* calculates the following assistant authentication message:
$hf_{b\text{-}a}=\{ID_{MS},a,b,ID_{f_1},\cdots,ID_{f_{L_3}},E_{K_{b-MS}}(f_1(b,a),\cdots,f_{L_3}(b,a))\}$.
If *b* receives the broadcast information of the MS, it sends $hf_{b\text{-}a}$ to the MS; otherwise, it request *a* to forward $hf_{b\text{-}a}$ to the MS.

Step 6. When MS receives $hf_{c\text{-}a}$ ($c\in Au_a$), it calculates the key $K_{MS\text{-}c}$ shared with *c*, and decrypts $hf_{c\text{-}a}$ with $K_{MS\text{-}c}$ getting $hK_{c-a}=f_1(c,a)\oplus\cdots\oplus f_{L_3}(c,a)$.

Step 7. MS evaluates $MAC_{AP_{c\text{-}a}}=H(hK_{c\text{-}a}, r_k+2)$ for each *c* ($c\in Au_a$) and sends them to *a*.

Step 8. For each node *c* ($c\in Au_a$), *a* recalculates $MAC_{AP_{a\text{-}c}}$ *with* $hK_{a\text{-}c}$ and r_k+2. If $MAC_{AP_{c\text{-}a}}=MAC_{AP_{a\text{-}c}}$, *c* is valid authentication node. Then, *a* finds out the valid authentication set EAu_a from Au_a. If $|EAu_a|<m$, *a* refuse to send data to MS; Otherwise, it can securely send data to MS. Their shard key is: $SK_{a\text{-}MS}=K_{a\text{-}MS}\oplus hK_{a\text{-}c_1}\oplus\cdots\oplus hK_{a\text{-}c_{m'}}$ ($c_j\in EAu_a$ and $m'=|EAu_a|$).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2770119, IEEE Wireless Communications Letters

III. Performance and Security Evaluation

In this section, we analyze the performance and security of our scheme, including local connectivity, MS replicated attack, and DoS attack.

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

1. We consider a SN deployed over fields of 1000m by 1000m. The number of a node's neighbors is 40.

2. The wireless communication range for a node is 40m.

3. The number of binary t-degree polynomials is 100, where *t* is 100.

A. Connectivity Analysis

The probability that any two nodes *a* and *b* can establish a shared key can be evaluated by the following equation:

$$P_{a-b} = 1 - \frac{\binom{n-t_2}{t_2}}{\binom{n}{t_2}} \tag{1}$$

The probability that an MS shares *x* polynomials with a sensor node is as follows:

$$P_x = \frac{\binom{n}{t_1}\binom{t_1}{x}\binom{n-t_1}{t_2-x}}{\binom{n}{t_1}\binom{n}{t_2}} = \frac{\binom{t_1}{x}\binom{n-t_1}{t_2-x}}{\binom{n}{t_2}} \tag{2}$$

Therefore, the probability of shared key being established between an MS and a sensor node is:

$$P_{MS-a} = \sum_{x_1=m}^{M} \binom{M}{x} \left(1 - \sum_{x=0}^{q-1} P_x\right)^{x_1} \left(\sum_{x=0}^{q-1} P_x\right)^{M-x_1} \tag{3}$$

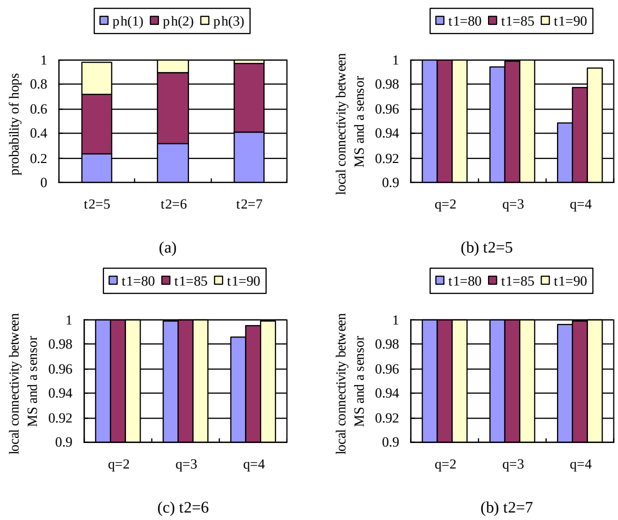


Figure 1. local connectivity.

Fig. 1 shows that the relationships between local connectivity and all parameters. In Fig. 1(a), we let *ph*(*l*) be the probability that the smallest number of hops needed to connect two neighboring nodes is *l*. Obviously, *ph*(l) is P_{a-b}. From figure 1 (a), we can observe that $ph(1) + ph(2) + ph(3) \approx 1$ when t2 is equal to or greater than 6. From the equation (1) to (3), we can find that P_{a-b} increases with the increase of *t*2, P_{MS-a} increases with the increase of t1 and *t*2 when values of *n*, *M* and *m* remain unchanged. The above conclusion can be verified by Fig. 1.

B. MS replicated attack

Resiliency of MS replicated attack, namely *RAP*, can be evaluated by the probability that an MS can collect data from uncompromised sensor nodes.

The probability that a polynomial may be compromised is:

$$RP_{KM} = 1 - \sum_{x=0}^{t} \binom{NC}{x} \left(\frac{t2}{n}\right)^{x} \left(1 - \frac{t2}{n}\right)^{NC-x} \tag{4}$$

The probability that a shared key between an MS and a sensor node may be compromised is:

$$RP_{MS-a} = \sum_{x_1=q}^{t2} \frac{P_{x_1}}{\sum_{x=q}^{t2} P_x} \left(RP_{KM}\right)^{x_1} \tag{5}$$

The probability that a shared key (includes keys established by key path) between two sensor nodes is compromised is:

$$RPh_{a-b} = 1 - \sum_{l_1=1}^{Th} \frac{ph(l_1)}{\sum_{l=1}^{Th} ph(l)} \left(1 - RP_{a-b}\right)^{l_1} \tag{6}$$

Where $RP_{a-b} = \sum_{x_1=1}^{t2} \frac{P'_{x_1}}{P_{a-b}} \left(RP_{KM}\right)^{x_1}$ (where $P'_{x_1} = \frac{\binom{t2}{x_1}\binom{n-t2}{t2-x_1}}{\binom{n}{t2}}$), *Th* is the maximum hops of key path required. Previous analysis indicates that *Th*=3 in our scheme.

The authentication model indicates that *RAP* can be evaluated by the following equation:

$$ARP = \begin{cases} RP_{MS-a}, & m' \geq m \\ RP_{MS-a} \cdot \left(RPh_{ab}\right)^{m-m'}, & m' < m \text{ and } m' + m'' \geq m \\ \left(RP_{MS-a}\right)^{1+m-m'-m''} \cdot \left(RPh_{ab}\right)^{m''}, & m' + m'' < m \end{cases} \tag{7}$$

where $m' = M \cdot CN / DN$, $m'' = CC \cdot M \cdot \pi \cdot R^2 / Ar$.

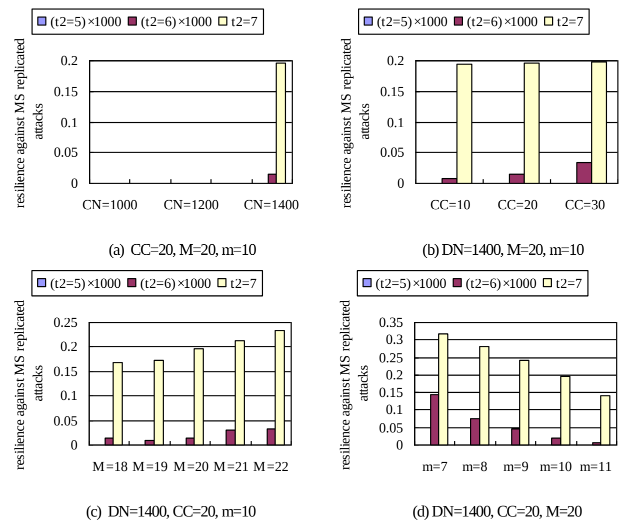


Figure 2. resilience against MS replicated attack. In the figure, t1=85 and ×1000 denotes the result is enlarged by 1000 times.

Fig. 2 shows those relationships between resilience against MS replicated attack and all parameter values. From the equations (5) to (7), we can find that *RAP* decreases with the increase of *t*2. But the equation (4) indicates that RP_{KM} significantly increases with the increase of *t*2. As a result, increasing *t*2 leads to a significant increase in *RAP*. This can be verified by Fig. 2. In this paper, nodes, compromised during the key establishment and delivery stage, stores key information received from their neighbors. Because RPh_{a-b} is less than RP_{MS-a}, *RAP* increases with the increase of *CC*. Fig. 2(b) can confirm this. The equation (7) shows that: 1. m' and m'' increase with the increase of *M*, which leads to the increase in *RAP*; 2. *RAP* decreases with the increase of *m*. For example, in Fig.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2770119, IEEE Wireless Communications Letters

2(d), when t2=7 and *m* increases to 11 from 7, *RAP* decreases to about 0.14 from 0.32.

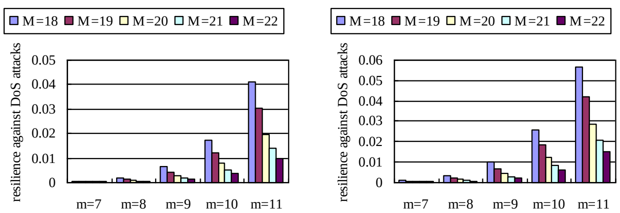
C. DoS attack

This kind of attack can lead normal MSs not to collect data from sensor nodes because of compromised nodes providing false authentication messages resulting in the number of valid authentication nodes collected by the sensor nodes is less than *m*. The resilience against DoS attack, namely *RDP*, can be evaluated by the probability that normal MSs cannot collect data from sensor nodes.

RDP can be evaluated by the following equation::

$$RDP = \begin{cases} 0, & CA + m \le M \\ \dfrac{\sum_{x_1 = M-m+1}^{\min(CA,M)} \binom{CA}{x_1}\binom{NA-CA}{M-x_1}}{\binom{NA}{M}}, & M < CA + m \le NA \\ 1, & CA + m > NA \end{cases} \quad (8)$$

where $CA = CN \cdot \pi \cdot R^2 / Ar$, $NA = DN \cdot \pi \cdot R^2 / Ar$.



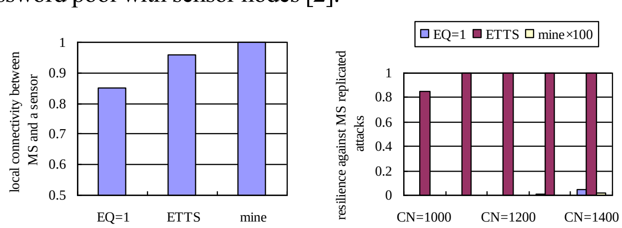
(a) CN=1200 (b) CN=1400

Figure 3. resilience against DoS attacks.

Fig.3 shows relationships between resilience against DoS attack and parameters. From the equation (8), we can draw the following conclusion: *RDP* increases with the increase of *CN*, and increases with the decrease of *M-m*. For example, when *M*=22 and *m*=10, *CN* increases to 1400 from 1200, *RDP* increases to about 0.006 from 0.004; when *M*=22 and *CN*=1400, *M-m* decreases to 11 from 15, *RDP* increases to about 0.015 from 0.0004.

D. Comparisons with Existing Schemes

In this subsection, performance of our scheme, ETTS scheme [2] and EQ scheme [8] is compared. In ETTS, nodes consist of static access nodes, MSs and sensor nodes. The number of a sensor node's neighbor static access nodes is 10. MSs share mobile key pool with static access nodes. Static access nodes share static key pool and the password pool with sensor nodes [2].



(a) (b)

Fig. 4 Comparing results. In (b), *CC*=10.

Fig. 4(a) shows the probability that an MS can establish pairwise key with a sensor node. In EQ, the above probability is low because pairwise key establishment between an MS and a sensor nodes is randomly selected from the sensor node's pre-distribution key ring by the sensor node. In our simulations, $P_{MS\text{-}a}$ in EQ is about 0.85. In ETTS scheme, MSs only can establish pairwise key with static access nodes with high probability. A sensor node can establish shared key with a static access node only when it shares at least one key space and a password with the static access node. Obviously, if a sensor node wants to establish pairwise key with an MS, it needs to the help of its one or two neighbor static access nodes to form a key path. In our simulations, $P_{MS\text{-}a}$ in ETTS and our scheme is about 0.96 and 1, respectively.

Fig. 4(b) shows the probability that a replicated MS can establish a pairwise key with an uncompromised sensor node. The research results in [2] indicate that: if a key space and some password keys are compromised, an attacker can successfully launch static access node replicated attack. In this paper, a replicated node can collect data from uncompromised nodes, is called mobile node replicated attack. In EQ, pairwise key establishment between an MS and a sensor node is randomly selected by the sensor node, which improves the resilience against MS replicated attack. In our scheme, multiple neighbors jointly authenticate MSs, which further improves the resilience against MS replicated attack. For example, when *CN*=1400, *ARP* of ETTS, EQ and our scheme is 1, 0.046, and 0.0001, respectively.

IV. Conclusion

In this paper, a (*M*,*m*) authentication scheme against MS replicated attacks is proposed. Analysis and simulation results indicate that: the greater the *M-m* is, the stronger the ability to resist DoS attack; the larger the *m* is, the stronger the ability to resist MS replicated attack. For example, when *M*=20, *m*=7, *n*=100, *t*=100, t1=85, t2=6, and *CN*=1400, the probability that a replicated MS can successfully collect data from uncompromised nodes is about 0.0001.

References

[1] R. Di Pietro, G. Oligeri, C. Soriente, et al., "United we stand: Intrusion-resilience in mobile unattended WSNs," IEEE Trans. Mobile Comput., vol. 12, no. 7, pp. 1456–1468, Jul. 2013.
[2] A. Rasheed, and R. N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with MSs," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 5, pp. 958-965, 2012.
[3] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proc. 2002 ACM CCS, pp. 243–254.
[4] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," IEEE Symp. Secur. Privacy, pp. 197-213, 2003.
[5] C. Blundo, A. D. Santis, A. Herzberg, "Perfectly-secure Key Distribution for Dynamic Conferences," Information and Computation, vol. 164, no. 1, pp. 1-23, 1998.
[6] P. Liu, P. Ning, "Establishing pairwise keys in distributed sensor networks," ACM Trans. on Information and System Security, vol. 8, no. 1, pp. 41-77, 2005.
[7] L. Lamport, "Password Authentication with Insecure Commuincation," Communications of the ACM, vol, 24, no. 11, pp. 770-772, November 1981.
[8] S. Li, W. Wang, B. Zhou, et al. A Secure Scheme for Heterogeneous Sensor Networks. IEEE Wireless Commun. Lett, vol. 6, no. 2, pp. 182-185, 2017.
[9] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: efficient security mechanisms for large-scale distributed sensor networks," ACM Trans. Sensor Networks, vol. 2, no. 4, pp. 500–528, 2006.