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.

II. OUR SCHEME

A. Notation and assumption

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

\[ f(x, y) = \sum_{i,j=0}^{q} a_{i,j} x^i y^j \]

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 \( r_1 \) and \( r_2 \) (\( 2 < r_1 \leq 1 \)) polynomials from the key pool, respectively. \( f(x,y) \) denotes the \( i \)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 \( L \geq 1 \) polynomials \( f_1(x,y), \ldots, f_L(x,y) \), 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 \( f_1(b,y), \ldots, f_k(b,y) \). At last, node \( b \) calculates the values \( f_1(b,a), \ldots, f_k(b,a) \), and sends the message \( U_{b-a} = \{a,b,E_{b-a}(inf),M_{b-a}\} \) (where \( inf = \{f_1(b,a),\ldots,f_k(b,a)\} \) ) to \( a \).

Step 3. When \( a \) receives \( U_{b-a} \), it decrypts \( U_{b-a} \) with \( K_{a-b} \) getting \( inf \) then it recalculates message authentication code \( M_{a-b} \). If \( M_{a-b} = M_{b-a} \), \( a \) 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, \( f_1(a, ID_{MS}), \ldots, f_L(a, ID_{MS}) \). If \( L > q \), determines the authentication set \( Au_a \) from \( CA_a \). If \( |Au_a| \geq m \), \( a \) sends a message \( inf_{a-MS} = \{ID_a, k, Au_a, ID_{MS}, \ldots, ID_{MS}\} \) (where \( k \) is the random number generated by \( a \)) to the MS. Otherwise, authentication between \( a \) and the MS fails.

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

Step 4. When \( a \) receives \( inf_{MS-a} \), it calculates their shared key \( K_{a-MS} \) 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 \( RA_a \), finds the polynomials, namely \( f_1(b,y), \ldots, f_L(b,y) \), shared with the MS. If \( L > q \), \( b \) calculates the following assistant authentication message:

\[ hf_{b-a} = \{ID_{MS}, a, b, ID_{MS}, \ldots, ID_{MS}, E_{K_{MS}}(f_1(b,a),\ldots,f_L(b,a))\} \]

If \( b \) receives the broadcast information of the MS, it sends \( hf_{b-a} \) to the MS; otherwise, it requests \( a \) to forward \( hf_{b-a} \) to the MS.

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

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

Step 8. For each node \( c \in Au_a \), \( a \) recalculates \( MAC_{AF_{c-a}} \) with \( hK_{c-a} \) and \( r_k + 2 \). If \( MAC_{AF_{c-a}} = MAC_{AF_{c-a}} \), \( c \) is valid authentication node. Then, \( a \) finds out the valid authentication set \( E_{Au_a} \) from \( Au_a \). If \( |E_{Au_a}| \leq m \), \( a \) refuses to send data to MS; Otherwise, it can securely send data to MS. Their shared key is:

\[ SK_{a-c} = K_{MS} \oplus hK_{a-1} \oplus \cdots \oplus hK_{a-c} \ (c_j \in E_{Au_a} \text{ and } m = |E_{Au_a}|) \].

---

**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_0 | The ID of the polynomial \( f_i(x,y) \) |
| ID_MS | The ID of MS |
| K_{a-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_{a}(inf) | The information \( inf \) is encrypted by symmetric encryption algorithm \( E \) with the key \( K \) |
| H_{a}(inf) | The MAC of the message \( inf \), which is generated by Hash with the key \( K \) |
| \( inf_1 \oplus inf_2 \) | Concatenating the message \( inf_1 \) and \( inf_2 \) |
| \( inf_1 \oplus inf_2 \) | XOR the information \( inf_1 \) and \( inf_2 \) |
| [S] | The size of set \( S \) |
### 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:

\[ P_{a-b} = 1 - \left( \frac{n-t}{t} \right) \left( \frac{n-t}{t} \right) \left( \frac{n-t}{t} \right) \left( \frac{n-t}{t} \right) \]  

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

\[ P_x = \left( \frac{n}{t} \right)^x \left( \frac{n-t}{t} \right)^{n-x} \]  

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

\[ P_{MS-a} = \sum_{m=x}^{M} \binom{M}{m} \left(1 - \sum_{x=0}^{q} P_x \right)^{M-x} \]  

where \( q = \frac{1000}{10000} \times 1000 \times 1000 \times 1000 \times 1000 \)

#### 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:

\[ RP_{KM} = 1 - \sum_{x=0}^{t} \binom{M}{x} \left( \frac{1}{n} \right)^x \left( 1 - \frac{t}{n} \right)^{M-x} \]  

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

\[ RP_{MS-a} = \sum_{x=0}^{t} \binom{M}{x} \left( \frac{1}{n} \right)^x \left( 1 - \frac{t}{n} \right)^{M-x} \]  

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

\[ RPh_{a-b} = 1 - \sum_{x=0}^{t} \binom{M}{x} \left( \frac{1}{n} \right)^x \left( 1 - \frac{t}{n} \right)^{M-x} \]  

where \( RPh_{a-b} = 1 - \sum_{x=0}^{t} \binom{M}{x} \left( \frac{1}{n} \right)^x \left( 1 - \frac{t}{n} \right)^{M-x} \)  

\( Th \) 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:

\[ ARP = \left( RPh_{a-b} \right)^{m\cdot m'} \]  

where \( m = M \cdot CN / DN \) and \( m' = CC \cdot M \cdot \pi \cdot R^2 / Ar \).

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, \( ph(l) = P_{a-b} \). From figure 1 (a), we can observe that \( ph(1) + ph(2) + ph(3) \approx 1 \) when \( t = 2 \) 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 \( t, P_{MS-a} \) increases with the increase of \( t \) when values of \( n, M \) and \( m \) remain unchanged. The above conclusion can be verified by Fig. 1.

**Fig. 1.** Local connectivity.

![Fig. 1](image-url)

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 \( t \). But the equation (4) indicates that \( RP_{KM} \) significantly increases with the increase of \( t \). As a result, increasing \( t \) 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.** Resilience against MS replicated attack. In the figure, \( t = 85 \) and \( C = 1000 \) denotes the result is enlarged by 1000 times.

![Fig. 2](image-url)
2(d), when $t_2=7$ 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:

$$
RDP = \begin{cases} 
0, & CA + m \leq M \\
\sum_{k=0}^{\min(CA, M)} \binom{CA}{k} \binom{M-CA}{M-k} \left( \frac{NA-CA}{M} \right)^k \left( \frac{CA}{M} \right)^{M-k}, & M < CA + m \leq NA \\
1, & CA + m > NA 
\end{cases}
$$

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

Fig. 4(a) shows the probability that an MS can establish a pairwise key with an uncompromised sensor node, which improves the resilience against MS replicated attack. In the simulations, $P_{MS-a}$ in EQ is about 0.85. In ETTS scheme, MSs 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 help its one or two neighbor static access nodes to form a key path. In our simulations, $P_{MS-a}$ 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 $M=20$, $m=7$, $n=100$, $t=100$, $t_1=85$, $t_2=6$, and $CN=1400$, the probability that a replicated MS can successfully collect data from uncompromised nodes is about 0.0001.

REFERENCES


