Secret-Sharing Approach for Detecting Compromised Mobile Sink in Unattended Wireless Sensor Networks

Xiangyi Chen(✉) and Liangmin Wang

School of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang, China
{chenxyzj, wanglm}@ujs.edu.cn

Abstract. In unattended wireless sensor networks (UWSNs), static sensor nodes monitor environment, store sensing data in memory temporally. Mobile sink patrols and collects the sensors' data itinerantly. Mobile sink is granted with more permissions than static sensor nodes, rendering it more attractive to the adversary. By compromising the mobile sinks, the adversary can not only seek the sensing data, but it also can steel all kinds of keys and access permissions, which may be abused to undermine other benign sensor nodes, even worse to upset the whole network. Currently, many related works focus on key management, permission management to restrict the compromised mobile sink or authentication to guarantee data reliability. However, the issue of compromised mobile sinks attracts little attention, and gradually become one obstacle to the application of UWSNs.

In this paper, we proposed a secret-sharing method for detecting compromised mobile sink in UWSNs. Before the sensing data are collected by the mobile sink, every sensor node splits the digest of its data into shares by using a polynomial secret sharing algorithm, and dispatches these secret shares to randomly chosen neighbor nodes, which thereafter send to the base-station through different routes. After enough shares are gathered, the base-station recovers the original data digest, which will be used to validate the sensing data submitted by the mobile sink. If the validation fails, it reveals a compromised mobile sink. Theoretical analysis and evaluation indicate the effectiveness and efficiency of our method. Also, we proposed two types of attacking model of the mobile adversary, and obtained the respective detection probability.

Keywords: Detecting · Compromised mobile sink · Secret sharing
Unattended wireless sensor networks

1 Introduction

Unattended wireless sensor networks [1–3] are deployed in monitoring environment or inaccessible enemy areas, such as volcanoes, battlefield, national borders and other places, for disaster monitoring, military espionage and tracking, intrusion early warning, etc. In an UWSN, static nodes accomplish tasks like sensing the environment and storing the monitoring data, the mobile sink (MS) periodically visits and gathers data from static

L. Zhu and S. Zhong (Eds.): MSN 2017, CCIS 747, pp. 303–317, 2018.
https://doi.org/10.1007/978-981-10-8890-2_22

nodes. And finally the mobile sink reports these data to the base-station (BS). Accordingly, the mobile sink can also help the base-station carry out other important tasks, such as time synchronization, session key update, network maintenance, etc.

The unattended nature makes UWSNs vulnerable to various kinds of attacks. Especially, the mobile sink is authorized to gather data, update session key, and other critical missions, therefore is the focus of attackers. With the compromised mobile sink, the adversary can grab, expurgates, falsifies, and even forge all the monitoring data, further can launch other more threatening attacks, such as, revoking the benign sensor nodes, desynchronizing network time, forging network routes and causing network topology division, etc. Besides, the adversary can also launch other insider attacks, for example eavesdropping, denial-of-sleep attack [4], sybil attack [5], sinkhole attack [6], replication attack [7–12], etc.

Although a few studies [13, 14] proposed some strategies to curtail the power of mobile sink in UWSN. Once the mobile sink was found compromised, the base-station limits or revokes the authorized permissions, preventing its subsequent destruction. However, there is little research on the detection of mobile sink. At present, current UWSN research mainly focus on the defense of compromised mobile sink and detection of compromised static nodes, leaving the detection of compromised mobile sink an open problem.

Focusing on the detection of the mobile sink in UWSN, this article proposed a method for detecting the compromised mobile sink based on secret sharing. As shown in Fig. 1, during every data collecting round of the mobile sink, every static node calculates the digest of its sensing data, splits the digest into multiple shares by using a polynomial secret-sharing algorithm. Then, these secret shares are sent to some randomly selected neighbor nodes, which will thereafter forward these secret shares to the central base-station. The base-station can recover the original data digest using the secret-sharing algorithm after receiving enough shares. At the end of the data aggregation round when the mobile sink submits the aggregated data to the base-station, the aggregated data and the data digest can be used to validate whether the mobile sink has ever tampered the sensors' data. If the validation fails, then the compromised mobile sink is detected.

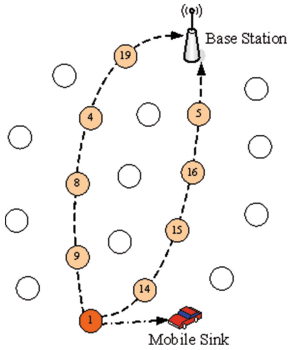


Fig. 1. Compromised mobile sink detection by using secret sharing

The rest of this article is organized as follows: Sect. 2 overviews some relevant works in the literature. In Sect. 3, the network model and security hypothesis are introduced. Further, Sect. 4 presents our detection method of the compromised mobile sink based on secret sharing. Section 5 analyzes and evaluates the performance of our method. Finally, Sect. 6 summarizes the whole work.

2 Related Works

Currently there are many works related to node compromise in wireless sensor networks, such as replication attack detection [7–12], node compromise detection [15–20] and physical capture detection [21–24].

2.1 Replication Attack Detection

Yu et al. [10] proposed XED method to detect replication attack in mobile sensor network. When two mobile sensor nodes meet they exchange two random numbers as their encounter evidence, which will be used as passphrases in their next meeting. If the passphrases authentication fails, replication attacks are detected. Although this approach is simple and effective, but it does not consider the collusion of multiple replica nodes. Kai et al. [11] proposed to detect replication attacks in MANETs, by means of conflicting nodes' location and time after local information interchange between mobile nodes in their meeting. Wang et al. [12] proposed to use mobile patroller to detect replication attacks. These studies [10–12] deal with the node replication issue instead of compromised mobile sink problem in UWSNs.

2.2 Compromised Static Nodes Detection

Taejoon et al. [15] proposed to detect compromised sensor nodes by verifying the node's program code. References [16–20] uses the message passing to verify node's program to detect the compromised node by the adversary.

2.3 Physical Capture Attacks Detection

Most studies assume that node capture is easy to implement and difficult to detect. However, Becher et al. [21] overturn this assumption by experiments, they found that it's not easy to conduct the physical capture attack. Apart from enough indispensible professional knowledge and expensive equipment, the sensor node must be taken offline for a period of time that cannot be ignored. Short attacks involve in creating plug-in connections and make data transfers takes about 5 min, the medium duration attacks involving welding or de-welding device consume more than 30 min, and the long duration attacks involving erasing the program security protection and modifying the code require at least several hours.

Based on Becher et al.'s work [21], Mauro et al. [22, 23] proposed to detect node capture attacks in MANETs by using mobility and collaboration, if the meeting interval exceeds a preset threshold, then the physical capture attacks is detected with large

probability. But this method is not applicable in sensor networks with static nodes. Ding et al. [24] proposed to determine whether the neighbor is online to detect physical capture attack by response messages after periodically sending hello message.

3 Network Model and Assumptions

In this section, we presents our network model and security assumptions. First, Table 1 lists the notations used in this article and their corresponding meaning.

Table 1. Notations and descriptions

Notation	Meaning
$\boldsymbol{Z}$	The identifiers set of static sensor nodes in network, $\boldsymbol{Z}$ = {1, 2, 3,…, N}
N_i	The neighbor nodes set of sensor node s_i
$\|N_i\|$	The neighbors number of sensor node s_i
U_i	The neighbors set chosen by sensor node s_i for sharing the secret
$\|U_i\|$	The number of the set U_i
d_i^r	Sensing data by node s_i in the r-th round
D_i	$\{d_i^r \mid 1 \leq r \leq \tau\}$, sensing data by node s_i in τ rounds
$h(.)$	One way hash function
τ	The hop count from secret share holder to the base-station
t_i	The threshold parameter in secret sharing chosen by node s_i
n_i	The total number of the secret shares split by node s_i
p_i	The prime number chosen by node s_i
Z_{p_i}	A finite field with order p_i
a_{ij}	$1 \leq j \leq t_i - 1, 0 \leq a_{ij} < p_i$, the j-th coefficient in node s_i's polynomial
M_i	Secret to be shared by node s_i
z_i	$z_i = h(M_i)$, the hash value of the secret of node s_i
$f_i(x)$	The secret-sharing polynomial of node s_i

3.1 Network Model

The unattended wireless sensor network consists of N static nodes, a mobile sink and one central base-station. The mobile sink periodically patrols around the network, collects the sensing data from every static sensor node and temporarily stores in its memory. At the end of one patrol round, the mobile sink submits all the data to the base-station.

3.2 Security Assumptions

It is assumed that the base-station and the mobile sink both have strong computing and storage capabilities, the public key algorithm between mobile sink and BS is used to implement encryption and signature to ensure confidentiality and integrity of data.

While, the static nodes have limited computing and storage capabilities, symmetric key algorithms are used for session keys between the base-station and the static nodes, between the mobile sink and the static nodes.

Also, we assume that the trusted central base station is located in a secure location, it will not be captured by the attacker, and however, both the mobile sink and the static nodes could be captured by the attacker. Once the mobile sink or any static node is captured, the attacker can acquire the node ID, the key, and the sensor data. The mobile sink, compared to the static sensor node, owns more credentials and aggregates the sensing data, attracts much more attention from the attacker. Therefore, the mobile sink will be the first target of the attacker. Thus, we focus on the detection of compromised mobile sink in this work.

In order to avoid triggering nodes offline defense mechanism [22–24], the captured sensor nodes will be released back into the network by the attacker, allowing the compromised nodes to participate in the network as if they are benign nodes. In addition, it is assumed that the number of nodes that the attacker can capture at a time is less than the total number of nodes of the network; otherwise all security mechanisms will fail.

4 Compromised Mobile Sink Detection by Using Secret Sharing

In this section, we first present the method to share secrets among static nodes. Then, the approach for the base-station to detect compromised mobile sink is proposed.

4.1 Secret Partition and Distribution

At the τ-th round, the static node acquires its sensing data, then it shares the secrets among its neighbors, which can be described as six steps in the following.

(1) Parameters selection
Sensor node s_i randomly chooses parameters t_i and n_i, which also meet $1 < t_i \leq n_i < |N_i|$. Then, it randomly chooses n_i neighbors as a subset, denoted by U_i, from its neighbors set N_i.

(2) Secret generation
Sensor node s_i calculate the secret to be shared M_i as Eq. (1).

$$\begin{aligned} &M_i = h(t_i \| k_1 \| \ldots \| k_l \| k_{l+1} \| \ldots \| k_{n_i} \| d_i^0 \| d_i^1 \| \ldots \| d_i^\tau) \\ &(k_l \in \mathrm{Z}, k_l < k_{l+1}) \end{aligned} \tag{1}$$

(3) Secret polynomial
Sensor node s_i selects a prime p_i which satisfies $p_i > \max(n_i, M_i)$. Then, $(t_i - 1)$ independent coefficients in the finite field Z_{p_i} are chosen at random, which is denoted by the set $\{a_{ij} | (1 \leq j \leq t_i - 1) \wedge (0 \leq a_{ij} < p_i)\}$, which are used to produce a $(t_i - 1)$-order secret sharing polynomial $f_i(x)$ as Eq. (2).

$$f_i(x) = (\sum_{j=1}^{t_i-1} a_{ij}x^j + M_i) \bmod p_i \tag{2}$$

(4) Secret splitting
In Eq. (2), x respectively takes the identifiers in the chosen neighbor subset U_i. After calculations, the identifiers and the respective secret shares can be expressed as a set $\{(k, y_{ik})|y_{ik} = f_i(k), k \in U_i\}$.

(5) Secret shares dispatching
Sensor node s_i sends the secret share y_{ik} to sensor node s_k, which would independently forwards such secret share to the base-station.

(6) Secrets deletion
Sensor node s_i deletes secret M_i, parameters t_i and n_i, as well as the coefficients set $\{a_{ij}\}$ and the polynomial $f_i(x)$, while it stores the prime number p_i and all its sensing data. The neighbor node will delete the secret share after sending it to the base station.

4.2 Compromised Mobile Sink Detection

(1) Mobile sink submits data to base-station
The mobile sink patrols around the network for collecting sensing data from the static nodes. For each node $s_i(1 \le i \le N)$, the mobile sink collects the sensing data D_i and the stored prime number p_i. Then, the sensor node removes such data from its memory and begins next sensing round. After all sensor nodes have been patrolled and data have been collected, the mobile sink submits the result $\{(D_i, p_i)|i \in Z\}$ to the base-station.

(2) Secret recovery
After receiving all the secret shares of sensor s_i, the base-station counts and gets the number n_i of total shares. Then, it recovers the secrets by means of polynomial interpolation.
As shown in Eq. (3), polynomial interpolation can be conducted in the point set $\{(k, y_{ik})|y_{ik} = f_i(k), k \in U_i\}$, which was composed by the secret shares from sensor s_i.

$$f_i(x) = \sum_{k \in U_i} y_{ik} \prod_{l \in U_i \wedge l \neq k} \frac{x-k}{l-k} \bmod p_i \tag{3}$$

Further, the base-station can restore the original secret as in Eq. (4). The secret sharing parameter t_i equals the highest exponent of polynomial (4) plus one.

$$M_i = f_i(0) = \sum_{k \in U_i} y_{ik} \prod_{l \in U_i \wedge l \neq k} \frac{k}{k-l} \bmod p_i \tag{4}$$

(3) Detecting the compromised mobile sink
With the identifier ID, the parameter t_i^r and the sensors' data submitted by the mobile sink, $h(t_i \| k_1 \| \ldots \| k_l \| k_{l+1} \| \ldots \| k_{n_i} \| d_i^0 \| d_i^1 \| \ldots \| d_i^\tau)(k_l \in D, k_l < k_{l+1})$ is calculated by the base-station. After comparing this digest with the restored corresponding value enclosed in the secret M_i, the base-station could judge whether the mobile sink has been compromised or not. If this verification fails, it implies the compromise of the mobile sink.

5 Analysis and Evaluation

In this section, we will analyze and calculate the detection overheads in computation, memory, communication and the detection efficiency. Also, the parameters selection and how these parameters affect the detection results will be discussed in details.

5.1 Detection Overheads

(1) Computation overhead
The main computation overhead of static sensor nodes is the modular exponential algorithm of the polynomial $f_i(x) = (\sum_{j=1}^{t_i-1} a_{ij}x^j + M_i) \bmod p_i$ in finite field. Since multiplication is more complex and computationally intensive than addition, the overall computation overhead can be approximated using the number of total multiplications. In the polynomial $f_i(x)$, there are total $(2t - 3)$ multiplications, which involve $(t - 2)$ multiplications in the modular exponentiation, and $(t - 1)$ multiplications in the products between the exponentiations and the coefficients. Therefore, the total computation cost is $O(n(2t - 3))$.
(2) Memory overhead
Every static sensor node splits its secret into n shares, and sends to randomly selected neighbors. Thus, the average memory overhead is $O(n)$.
(3) Communication overhead
The n secret shares are forwarded to the base-station through different routes by the randomly selected neighbors. The average number of hops in those routes is $O(\sqrt{N})$ [25], so the communication cost of every sensor node are $O(n\sqrt{N})$.

5.2 Performance Analysis and Parameters Setting

We first consider an adversary that can only compromise one sensor node during the period of the share forwarding between two neighbors. Based on this attacking model, analysis and evaluations are detailed as to the detection efficiency. we analyze and discuss how to increase the detection efficiency and lower the detection overheads. Finally, we consider the more powerful adversary which can compromise more than

one sensor nodes in one-hop communication interval. The detection efficiency against such adversary is deduced and discussed with different parameters.

(1) **Only one static sensor node compromised in one round**

We supposed an adversary with the knowledge of the network topology, the defense strategy and the intrusion detection methods. But the adversary is unaware of the secret sharing parameters t and n due to the randomness. As a consequence, in order to compromise the original secret, the adversary would have to recovery the secret after compromising as much secret shares as possible.

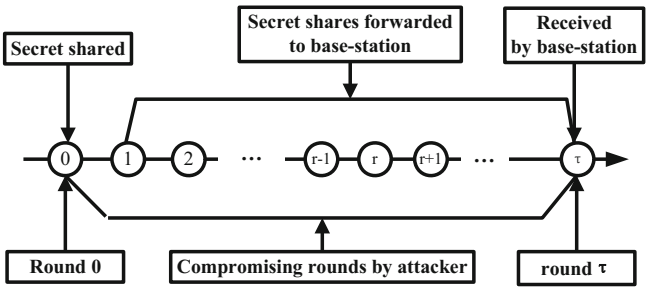


Fig. 2. Node compromised by adversary

In Fig. 2, we assume the average forwarding hops from the static sensor nodes to the base-station is τ. Also, it is assumed that the adversary can only compromise one sensor node in one hop communication. Then before the secret shares of the message digest reach the base-station, there are τ rounds for the adversary to compromise static sensor nodes.

Definition 1. $S = \{s, f\}$ is a sample set with only two elements, s indicates that the compromised sensor node is a secret shareholder, while f indicates that the compromised sensor node does not own a secret share.

Definition 2. X is a random variable with (0–1) distribution defined in the sample space. It represents the result after one round attack by the adversary, just as in Eq. (5).

$$X = X(e) = \begin{cases} 0, when & e = f \\ 1, when & e = s \end{cases} \tag{5}$$

In one round of compromise, the adversary captures one sensor node. This can be regarded as one random experiment with two possible results: the sensor node has the secret share holder or not. Before the secret shares are forwarded to the base-station, there are τ attempts for the adversary to compromise.

Let Y denotes the number of experiments with result $\{X = 1\}$ in τ rounds random experiments. That is, the number of total secret shares compromised by the attacker in τ

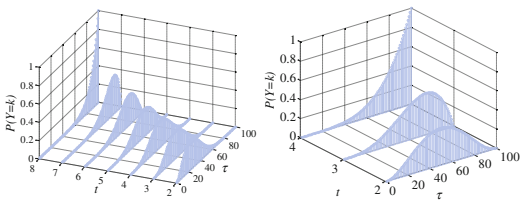
rounds. The domain of Y should be $[\max(0, \tau + n - N), \min(n, \tau)]$, and the probability of the event $\{Y = k\}$ can be expressed as Eq. (6).

$$P\{Y = k\} = p_k, k \in [\max(0, \tau + n - N), \min(n, \tau)] \tag{6}$$

Equation (6) is the probability distribution of the random variable Y. If the compromised sensor node doesn't hold the desired secret share, then it will be released to the network by the attacker lest this attack alarms the off-line intrusion detection mechanism. Later, the adversary chooses other compromising sensor node from the remaining sensor nodes. This attacking model can be modeled as sampling without replacement, or the "urn problem". In a network whose total number of sensor nodes is N, the number of the desired secret shares is n, while only t shares are needed to recover the original desired secret. There are τ attempts for the adversary to compromise. The event that the number of the success compromise equals k is denoted by $\{Y = k\}$. Let $\boldsymbol{P}\{Y = k\}$ be the probability of this event. Then the random variable Y obeys the hyper geometric distribution with parameters (N, n, τ). The distribution law can be expressed as Eq. (7).

$$P\{Y = k\} = \frac{C_n^k C_{N-n}^{\tau-k}}{C_N^\tau}, k \in [\max(0, \tau + n - N), \min(n, \tau)] \tag{7}$$

Figure 3 illustrates how $P\{Y = k\}$ changes in two cases with different parameter setting. In Fig. 3(a), N = 100 and n = 8, when parameter t changes from 2 to 8, the probability that the adversary compromises k secret shares decreases gradually. However, if the number of compromised sensor nodes increases from 0 to 100, the probability will gradually become larger. Figure 3(b) reveals a similar trend.



(a). N=100,n=8 (b). N=100,n=4

Fig. 3. $P\{Y = k\}$ varies with parameter t and τ

If the adversary wants to tamper the sensing data by compromising the mobile sink, he must compromise at least t sensor nodes which also own t secret shares. Therefore, we can define the false negatives of compromised mobile sink as follows.

Definition 3. The false negative of compromised mobile sink detection is defined as an event that the compromised mobile sink is not detected (**CMU**: Compromised Mobile sink Undetected), that is the adversary compromised at least t sensor nodes which own

the respective secret shares. The probability is defined as false negative of the detection.

Let **CMU** = $\{Y >= t\}$ be the false negative event, and $\boldsymbol{P_{cmu}}$ be the false negative, and then we obtain Eq. (8).

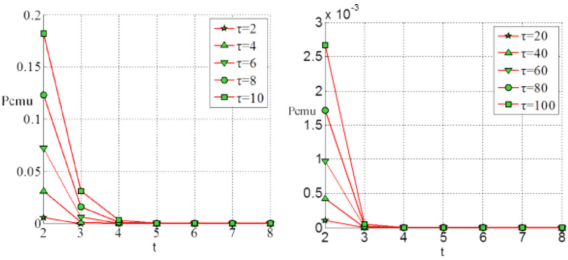
$$\begin{aligned} P_{cmu} &= P\{Y > \ = t\} \\ &= P\{Y = t\} + P\{Y = t+1\} + \ldots + P\{Y = \min(n, \tau)\} \\ &= \sum_{j=t}^{\min(n,\tau)} P\{Y = j\} \end{aligned} \tag{8}$$

In Eq. (8), when $j > \min(n, \tau)$, then we have $P\{Y = j\} = 0$. So, Eq. (8) can be further regarded as Eq. (9).

$$\begin{aligned} P_{cmu} &= P\{Y \geq t\} \\ &= P\{Y = t\} + P\{Y = t+1\} + \ldots + P\{Y = \min(n, \tau)\} + \ldots \\ &= \sum_{j=t}^{\infty} P\{Y = j\} \\ &= \frac{C_{\tau}^{t} C_{N-\tau}^{n-t}}{C_{N}^{n}} {}_3F_2\left[\begin{matrix} 1, n-t, \tau-t \\ t+1, N+t+1-n-\tau \end{matrix}; \quad 1\right] \end{aligned} \tag{9}$$

In Eq. (9), ${}_3F_2\left[\begin{matrix} 1, n-t, \tau-t \\ t+1, N+t+1-n-\tau \end{matrix}; \quad 1\right]$ is a hyper geometrical series.

When N and τ are fixed, the false negatives are determined by parameter t and n. Figure 4 shows the false negatives of our detection method in two scenarios. In Fig. 4 (a) with $N = 100$, $n = 8$, and the average hops of the network $\tau = \sqrt{\mathrm{N}} = 10$, the false negatives will be less than 5% when $t \geq 3$; while in Fig. 4(b) with $N = 10000$, $n = 8$, and the average hops of the network $\tau = \sqrt{\mathrm{N}} = 100$, the false negatives will be less than 0.3% when $t = 2$.



(a). N=100,n=8 (b). N=10000,n=8

Fig. 4. False negatives in two scenarios

If after τ rounds of attacks, the count of the compromised sensor nodes which own the secret shares is less than t, then the compromised mobile sink would be detected. So, we can define the compromised mobile sink detected event and its probability as follows.

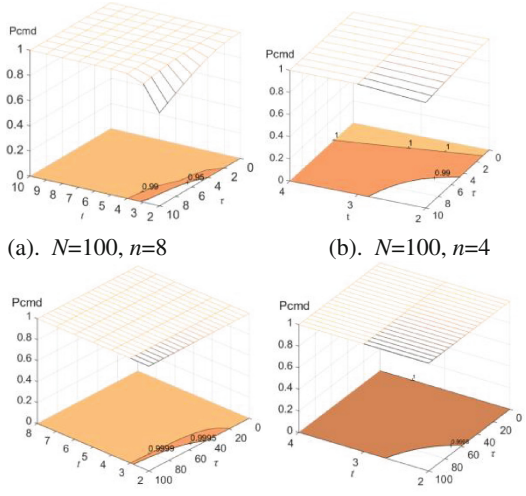
Definition 4. The compromised mobile sink detected event is defined as **CMD** (compromised-mobile sink-detected), that is the adversary compromised less than t sensor nodes which own the secret shares.

Let **CMD** = $\{Y < t\}$ be the detection event, and $\boldsymbol{P_{cmd}}$ be the probability, and then we obtain the Eq. (10).

$$\begin{aligned} P_{cmd} &= P\{Y<t\} = P\{Y=0\} + P\{Y=1\} + \ldots + P\{Y=t-1\} \\ &= \sum_{j=0}^{t-1} P\{Y=j\} = 1 - P\{Y \geq t\} \\ &= 1 - \frac{C_{\tau}^{t} C_{N-\tau}^{n-t}}{C_{N}^{n}} {}_3F_2\left[\begin{matrix} 1, n-t, \tau-t \\ t+1, N+t+1-n-\tau \end{matrix}; \quad 1\right] \end{aligned} \tag{10}$$

When N and n are fixed, the detection probability $\boldsymbol{P_{cmd}}$ is determined by secret sharing parameters t and τ. Figure 5 shows four cases of detection probability with parameters t and τ.

As shown in Fig. 5, if N is fixed, the average hops of the network are $\sqrt{\mathrm{N}}$, so $1 \leq \tau \leq \sqrt{\mathrm{N}}$. In Fig. 5(a), the detection probability is greater than 80% when N = 100 and n = 8. Figure 5(b) shows the detection probability exceeds 95% even if n is reduced to 4 with N = 100. Similarly, in Fig. 5(c) and (d) with total sensor number N = 10000, the detection probabilities are both greater than 99% for n = 8 and n = 4. Also, it is shown that the secret sharing parameters n and t have little influence on the



(a). N=100, n=8 (b). N=100, n=4

(c). N=10000,n=8 (d). N=10000, n=4

Fig. 5. Detection probability

detection probability when $N \gg \tau$. Therefore, under such circumstances, in order to decrease the detection overheads, parameters t and n should take smaller values.

(2) **More than one node captured in one round**

In this subsection, we consider a more powerful adversary, which can compromise ρN nodes; ρ is a proportional factor between 0 and 1.

If in the r-th round, the probability that all the secret shares are acquired by the adversary is P_r, then the probability that the adversary couldn't obtain the secret until the r-th round can be calculated in Eq. (11).

$$P = (1 - P_1)(1 - P_2)\ldots(1 - P_{r-1})(1 - P_r) = \prod_{i=1}^{r}(1 - P_i) \tag{11}$$

The secret shares owned by the sensors in the $(r - 1)$-th round are forwarded to the its' next-hop sensors in the r-th round. If all the secret shares are not grabbed in the $(r - 1)$-th round, the adversary has to carry out the same capture attack in the r-th round. So, the probability that all secret shares are grabbed by the adversary is equal in every round, as shown in the Eq. (12).

$$P_1 = P_2 = \ldots = P_{r-1} = P_r \tag{12}$$

The probability in the Eq. (12) can be calculated as Eq. (13).

$$\begin{aligned} P_1 &= \frac{C_n^n C_{N-n}^{\rho N-n}}{C_N^{\rho N}} = \frac{C_{N-n}^{\rho N-n}}{C_N^{\rho N}} \\ &= \frac{(N-n)!}{(\rho N-n)!(N-\rho N)!} \times \frac{\rho N!(N-\rho N)!}{N!} \\ &= \frac{\rho(\rho N-1)\ldots(\rho N-n+1)}{(N-1)\ldots(N-n+1)} \end{aligned} \tag{13}$$

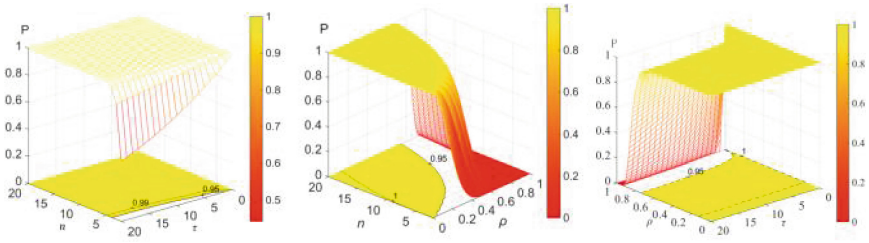
When $N \gg n$, Eq. (13) can be approximated as Eq. (14).

$$P_1 \approx \frac{\rho(\rho N)\ldots(\rho N)}{N\ldots N} = \rho^n \tag{14}$$

Finally, we obtain the approximation Eq. (15) about the Eq. (11).

$$P = (1 - P_1)^r \approx (1 - \rho^n)^r \tag{15}$$

Figure 6 shows this detection probability varies with the three parameters n, τ and ρ. In Fig. 6(a), N is fixed to 400 and $\rho = 20\%$, the detection probability approximates 100% when n is greater than 5. Figure 6(b) shows that when $\tau = 20$, even if half of the sensor nodes are compromised ($\rho = 20\%$), the detection probability still approximates 100% as long as $t = n > 10$. As illustrated in Fig. 6(c), if $t = n = 10$, the detection probability approaches 100% even if the adversary compromises $\rho = 50\%$ sensor nodes.



(a) ρ=20% (b) τ=20 (c) n=t=10

Fig. 6. Detection probability

6 Conclusion

In this paper, we proposed a compromised mobile sink detection scheme by using secret sharing. Every sensor node first splits the digest of its sensing data into shares by using a polynomial secret sharing algorithm, and then the secret shares are sent to the base-station through different routes by the sensor's neighbors. Finally, the base-station receives the shares, and then recovers the original data digest, compares with the data submitted by the mobile sink. Any difference reveals the compromised mobile sink, results in the detection by the base-station. Theoretical analysis and evaluation shows the effectiveness and efficiency of our method, the detection overheads are small. Also, the upper limit of detection probability was computed with the proposed compromise model of the mobile adversary.

Acknowledgment. This work is supported by the National Natural Science Foundation of China under Grant No. 61272074 and No. U1405255, the Key Research & Development Project of Jiangsu Province under Grant No. BE2015136, and the Industrial Science and Technology Foundation of Zhenjiang City under Grant No. GY2013030.

References

1. Khan, A.W., Abdullah, A.H., Anisi, M.H., Bangash, J.I.: A comprehensive study of data collection schemes using mobile sinks in wireless sensor networks. Sensors **2014**(14), 2510–2548 (2014)
2. Di Pietro, R., et al.: Data security in unattended wireless sensor networks. IEEE Trans. Comput. **58**(11), 1500–1511 (2009)
3. Reddy, S.K.V.L., Ruj, S., Nayak, A.: Distributed data survivability schemes in mobile unattended wireless sensor networks. In: Global Communications Conference (GLOBECOM 2012), Anaheim, California, USA, pp. 979–984. IEEE Press (2012)
4. Chen, C., Gao, X.B., Pei, Q.Q., et al.: A tactics to alleviate influence of denial-of-sleep attack in WSN. J. Jiangsu Univ. Nat. Sci. Ed. **31**(5), 570–575 (2010)
5. Douceur, J.R.: The sybil attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, pp. 251–260. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45748-8_24

6. Culpepper, B.J., Tseng, H.C.: Sinkhole intrusion indicators in DSR MANETs. In: Proceedings of 1st International Conference on Broadband Networks (Broad-Nets 2004), San Jose, California, USA, pp. 681–688. IEEE Press (2004)
7. Khan, W.Z., Aalsalem, M.Y., Saad, N.M.: Distributed clone detection in static wireless sensor networks: random walk with network division. PLoS One **10**(5), e0123069 (2015)
8. Mishra, A.K., Turuk, A.K.: Node coloring based replica detection technique in wireless sensor networks. Wirel. Netw. **20**(8), 2419–2435 (2014)
9. Contia, M., Pietro, R., Di Spognardic, A.: Clone wars: distributed detection of clone attacks in mobile WSNs. J. Comput. Syst. Sci. **80**(3), 654–669 (2014)
10. Yu, C.M., Lu, C.S., Kuo, S.Y.: Mobile sensor network resilient against node replication attacks. In: Proceedings of the 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON 2008), San Francisco, USA, pp. 597–599. IEEE Press (2008)
11. Xing, K., Cheng, X.: From time domain to space domain: detecting replica attacks in mobile ad hoc networks. In: Proceedings of the IEEE INFOCOM 2010, San Diego, CA, USA, pp. 1–9. IEEE Press (2010)
12. Wang, L.M., Shi, Y.: Patrol detection for replica attacks on wireless sensor networks. Sensors **2011**(11), 2496–2504 (2011)
13. Song, H., Zhu, S., Zhang, W., et al.: Least privilege and privilege deprivation: toward tolerating mobile sink compromises in wireless sensor networks. ACM Trans. Sens. Netw. (TOSN), **4**(4) (2008). Article 23
14. Liu, Z., Ma, J., Park, Y., et al.: Data security in unattended wireless sensor networks with mobile sinks. Wirel. Commun. Mob. Comput. **12**(13), 1131–1146 (2012)
15. Park, T., Shin, K.G.: Soft tamper-proofing via program integrity verification in wireless sensor networks. IEEE Trans. Mob. Comput. **4**(3), 297–309 (2005)
16. Du, X.: Detection of compromised sensor nodes in heterogeneous sensor networks. In: Proceedings of the IEEE 2008 International Conference on Communications (ICC 2008), Beijing, China, pp. 1446–1450. IEEE Press (2008)
17. Yang, Y., Wang, X., Zhu, S., et al.: Distributed software-based attestation for node compromise detection in sensor networks. In: Proceedings of 26th IEEE International Symposium on Reliable Distributed Systems, Beijing, China, pp. 219–230. IEEE Press (2007)
18. Krauß, C., Stumpf, F., Eckert, C.: Detecting node compromise in hybrid wireless sensor networks using attestation techniques. In: Stajano, F., Meadows, C., Capkun, S., Moore, T. (eds.) ESAS 2007. LNCS, vol. 4572, pp. 203–217. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73275-4_15
19. Jin, X., Putthapipat, P., Pan, D., et al.: Unpredictable software-based attestation solution for node compromise detection in mobile WSN. In: Proceedings of the IEEE 2010 GLOBECOM Workshops (GC Wkshps), Miami, Florida, USA, pp. 2059–2064. IEEE Press (2010)
20. Sei, Y., Ohsuga, A.: Need only one bit: light-weight packet marking for detecting compromised nodes in WSNs. In: Proceedings of the 7th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2013), Barcelona, Spain, pp. 134–143. IARIA (2013)
21. Becher, A., Benenson, Z., Dornseif, M.: Tampering with motes: real-world physical attacks on wireless sensor networks. In: Clark, J.A., Paige, R.F., Polack, F.A.C., Brooke, P.J. (eds.) SPC 2006. LNCS, vol. 3934, pp. 104–118. Springer, Heidelberg (2006). https://doi.org/10.1007/11734666_9

22. Conti, M., Di Pietro, R., Mancini, L.V., et al.: Emergent properties: detection of the node-capture attack in mobile wireless sensor networks. In: Proceedings of the First ACM Conference on Wireless Network Security, Alexandria, Virginia, USA, pp. 214–219. ACM (2008)
23. Conti, M., Di Pietro, R., Mancini, L.V., et al.: Mobility and cooperation to thwart node capture attacks in manets. EURASIP J. Wirel. Commun. Network. **2009**(1), 945943 (2009)
24. Ding, W., Yu, Y., Yenduri, S.: Distributed first stage detection for node capture. In: Proceedings of 2010 IEEE GLOBECOM Workshops (GC Wkshps), Miami, USA, pp. 1566–1570. IEEE Press (2010)
25. Dimitriou, T., Sabouri, A.: Pollination: a data authentication scheme for unattended wireless sensor networks. In: Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2011), Changsha, China, pp. 409–416. IEEE Press (2011)