Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks

Chia-Mu Yu[§†], Chun-Shien Lu[§*], and Sy-Yen Kuo[†]
[§]Institute of Information Science, Academia Sinica, Taipei, Taiwan 115, ROC
[†]Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 106, ROC

***Abstract*—In this paper, we study the challenging problem of node replication detection. Although defending against node replication attacks demands immediate attention, only a few solutions were proposed. In this paper, an Efficient and Distributed Detection (EDD) scheme and its variant, SEDD, are proposed to resist against node replication attacks in mobile sensor networks. The characteristics possessed by EDD and SEDD include (1) Distributed Detection; (2) Efficiency and Effectiveness; (3) Individual Detection; (4) Network-Wide Revocation Avoidance. Performance comparison with known methods are provided to demonstrate the efficiency of the EDD and SEDD schemes.**

I. Introduction

Sensor networks could be used in applications such as environment monitoring and object tracking. Recently, due to the advance in robotics, mobile sensor networks become feasible and applicable.

Node Replication Attacks. Usually, the sensor networks are unattended and the sensor nodes are not equipped with the tamper-resistance hardware so that the adversary can capture one sensor node, fabricate many replicas having the same identity (ID) with the captured node, and then place these replicas back into the strategic positions in the network for further malicious activities. This is the so-called *node replication attack*. Since the credentials of replicas are all the clones from the captured node, the replicas can be considered as legitimate members of the network, which make detection difficult. From the security point of view, the node replication attack is considerably harmful to the networks because the replicas, which have legitimate keys and are controlled by the adversary, can easily launch the insider attacks without easily being detected.

Based on the requirement that each node must broadcast a signed location claim of itself to its neighbors at a certain synchronized time, most of the existing distributed detection schemes such as Broadcasting [11], DM [11], RM [11], LSM [11], SDC [18], P-MPC [18], and RED [3], adopt the *witness finding* strategy, in which each node finds a set of sensor nodes somewhere as the *witnesses* for checking whether there are the same IDs used at different locations, for replica detection. The protocol proposed in [14] detects the replicas by exploiting the fact that the set of neighbors of each node should be fixed. If certain keys are pre-distributed in the sensor nodes, the increased key usage for certain keys used by replicas can be a signal indicating the existence of replicas [1]. In [5], the non-emptiness of two exclusive subsets of sensor nodes' IDs also indicates that replicas are involved in the networks. All the aforementioned detection schemes are designed only for static networks. With the assumption that the replicas cannot collude together, Yu *et al*. [17] present a challenge-and-response strategy to construct the first distributed replica detection scheme, XED, for mobile sensor networks. Ho *et al*. [9] also propose a detection scheme for mobile sensor networks by using sequential probability ratio test. However, the effectiveness of Ho *et al*.'s scheme relies on the involvement of the base station, easily incurring the problems of single-point failure and fast energy depletion of the sensor nodes around the base station.

As a whole, it is found that only few schemes are proposed for mobile sensor networks. Even worse, they all rely on unrealistic assumptions. With the consideration of nodes' mobility and the distributed nature of sensor networks, it is desirable, but very challenging, to have an efficient distributed scheme for detecting replicas in mobile sensor networks.

Contributions. To detect the node replicas in mobile sensor networks, an Efficient and Distributed Detection (EDD) scheme and its variant, SEDD, scheme are proposed. EDD and SEDD possess the following characteristics. 1) *Distributed Detection*: EDD and SEDD can resist against the node replication attacks in a distributed fashion without involving the base station. 2) *Individual Detection*: Each node in the EDD and SEDD schemes is able to detect replicas by itself. 3) *Network-Wide Revocation Avoidance*: The revocation of the replicas can be performed by each node without flooding the revocation messages to the entire network. 4) *Efficiency and Effectiveness*: The EDD and SEDD schemes can identify the replicas with high detection accuracy. In addition, their communication overhead is only $O(1)$ in the average case but is $O(n)$ in the worst case.

II. System Model

Network Model. Assume that the sensor network consists of n sensor nodes with IDs, $\{1, \ldots, n\}$. The communication is assumed to be symmetric. In addition, each node is assumed to periodically broadcast a beacon containing its ID to its neighbors. This is usually required in various applications, for example, object tracking. After the nodes are deployed to the sensing field, the time is divided into time intervals, $T_1, T_2, \ldots$, each of which has the same length T. In EDD and SEDD, the sensor nodes have mobility and move according to

*Contact Author: Dr. C. S. Lu (lcs@iis.sinica.edu.tw).

978-1-4244-2515-0/09/$25.00 ©2009 IEEE

the random waypoint model [10], which is commonly used in ad hoc networks and have been adopted in [8], [16], [19]. In this model, each node randomly chooses a destination point in the sensing field, and then moves toward it with velocity v randomly selected from a pre-defined interval $[v_{min}, v_{max}]$. After reaching the destination point, the node remains static for a random time and then starts moving again according to the same rule. Finally, the common assumptions, including (i) each node is aware of its location and (ii) the network utilizes an identity-based public key system so that signature generation/verification is feasible, are made.

Security Model. In our methods, sensor nodes are not tamper-resistant. In other words, the corresponding security credentials can be accessed after sensor nodes are physically captured. We assume that sensor nodes could be captured by the adversary immediately after the sensor deployment; *i.e.*, there is no secure bootstrapping time available after the sensor deployment. Replicas have all the legitimate credentials from the captured nodes. Replicas are assumed to achieve *simultaneous collusion*, which implies they can communicate with each other without incurring time delay. We assume that the adversary cannot create a new ID because it is difficult for the adversary to have the corresponding security credentials. Since the existence of more replicas implies the easier detection, we only deal with the most difficult case, where only two replicas exists in the networks. It should be noted that the most challenging problem, *i.e.*, only single one replica exists in the network, is not considered in the existing methods [1], [3], [5], [9], [11], [14], [17], [18] and this paper.

III. The Proposed Method

A. The Efficient and Distributed Detection (EDD) Scheme

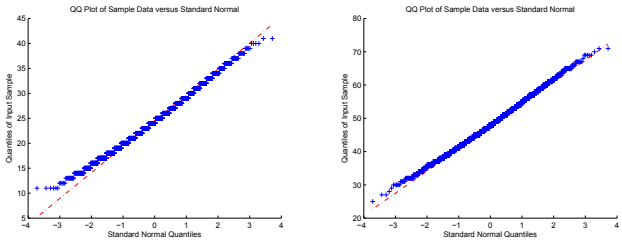
Basic Idea. The idea behind EDD and SEDD is motivated from the following observations. For a network without replicas, the number of times, μ_1, that the node u encounters a specific node v, should be limited in a given time interval of length T with high probability. For a network with two replicas v, the number of times, μ_2, that u encounters the replicas with the same ID v, should be larger than a threshold within the time interval of length T. According to these observations, if each node can discriminate between these two cases, each node has the ability to identify the replicas.

The EDD scheme is composed of two steps: off-line step and on-line step. The off-line step is performed by the network planner before the sensor deployment. The goal is to calculate the parameters, including the length T of the time interval and the threshold ψ used for discrimination between the genuine nodes and the replicas. On the other hand, the on-line step will be performed by each node per move. Each node checks whether the encountered nodes are replicas by comparing ψ with the number of encounters at the end of a time interval.

Off-line Step. The off-line step of EDD is shown in Fig. 1. The list $\mathcal{L}$ is used to store the number of encounters with every other nodes in a given time interval while the set $\mathcal{B}$ contains the IDs having been revoked. Let μ_1 and μ_2 be the random variables representing the expected number of encounters with the genuine nodes and replicas, respectively. Let σ_1^2 and σ_2^2 be the corresponding variances, respectively. The details of calculating μ_1, μ_2, σ_1^2 and σ_2^2 will be described in Sec. III-C. The 8th line of Fig. 1 is used to calculate the maximum possible number of encounters with the genuine nodes and the minimum possible number of encounters with the replicas. The parameter ϕ is used to control the trade-off between the efficiency and the detection accuracy, and is usually set to be 3. Here, an intrinsic assumption for the calculation of Y_1 and Y_2 is the model regarding the number of encounters within a given interval, whose normality can be validated in Figs. 2 and 3. The calculation provided in Sec. III-C can also give insight of supporting the normality. Different lengths of time intervals will result in different separability between the distributions of μ_1 and μ_2. Since the length T of the time interval is positively proportional to both the time required to detect the replicas and the storage overhead, T is required to be the smallest value such that each node can distinguish the replicas from the genuine nodes; *i.e.*, $Y_1 < Y_2$. Note that in some cases, the setting of $Y_1 > Y_2$ is possible because the network planner would like to compromise between the detection efficiency and detection accuracy.

Algorithm: EDD-Off-line-Step
1 select ϕ, φ and χ
2 $T = 1, \Omega = \emptyset, \mathcal{L} = \emptyset, \mathcal{B} = \emptyset, \Lambda = \emptyset$
3 $\Lambda_j = \emptyset, 1 \leq j \leq \varphi$
4 $D_j = \emptyset, 1 \leq j \leq \chi$
5 **repeat**
6 $T = T + 1$,
7 calculate μ_1, μ_2, σ_1^2, and σ_2^2
8 $Y_1 = \mu_1 + \phi\sigma_1$ and $Y_2 = \mu_2 - \phi\sigma_2$
9 calculate ψ
10 **until** $Y_1 < Y_2$

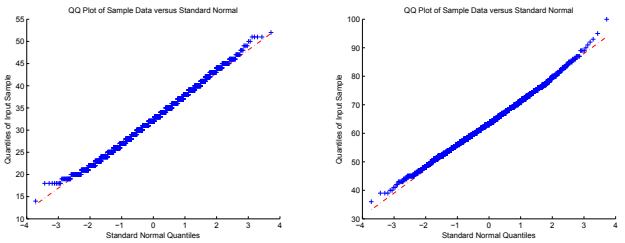
Fig. 1. Off-line step of the EDD scheme.



(a) (b)

Fig. 2. Q-Q plot in the setting of 9000 moves: (a) 0 replicas/comm. range is 30; (b) 2 replicas/comm. range is 30.

On-line Step. The on-line step of the EDD scheme is shown in Fig. 4, in which all the messages exchanged should be signed unless specifically noted. Each node locally maintains a counter t to record the elapsed time after the beginning of each time interval. After T time units is reached, *i.e.*, $t > T$, the counter t should be reset (lines 20 $\sim$ 21). Every time a node encounters the other node, the corresponding value in the list $\mathcal{L}$ (line 10) is increased. For example, when $t = 324$ and $\mathcal{L}[12] =$



(a) (b)

Fig. 3. Q-Q plot in the setting of 12000 moves: (a) 0 replicas/comm. range is 30; (b) 2 replicas/comm. range is 30.

19 is set by a certain node, it means that this node encounters the node 12 nineteen times by time unit 324 in a time interval. The node v can be revoked by u at any time as long as $\mathcal{L}[v]$ is above the threshold ψ (line 15). This is because from the normality point of view it is highly unlikely that the number of encounters with node v will be larger than ψ. The lines 10, 15, 20, and 21 realize the basic idea mentioned in Sec. III-A. However, since the effectiveness of EDD relies on the fact that each node periodically broadcasts its ID, the replicas may try to emulate the genuine nodes by using selective broadcast. The parts other than the lines $10, 15, 20$, and 21 in Fig. 4 are used to guarantee that the replicas also involve periodical broadcast. Otherwise, they will be detected and then revoked. This will be discussed in more details in Sec. IV.

Algorithm: EDD-On-line-Step
Condition: assume that this algorithm is performed by the node u at time t_i and $\{s_1, \ldots, s_d\}$ are the neighbors of u which are not in the set $\mathcal{B}$

1 broadcast a beacon $b_{u,i} = (u, \vec{w}_u, t_i)$
2 **if** $t \leq T$
3 $t = t + 1$
4 receive $b_{s_1,i}, \ldots, b_{s_d,i}$
5 **if** $\Omega \cap \{s_1, \ldots, s_d\} \neq \Omega$
6 flood $(u, \Omega \setminus \{s_1, \ldots, s_d\}, L_u, t_i)$
7 **if** $\Lambda \cap \{s_1, \ldots, s_d\} \neq \emptyset$
8 flood $(u, \Lambda \cap \{s_1, \ldots, s_d\}, L_u, \vec{w}^D_{\Lambda \cap \{s_1,\ldots,s_d\}}, t_i)$
9 **for** $\kappa = 1$ to d
10 $\mathcal{L}[s_\kappa] = \mathcal{L}[s_\kappa] + 1$
11 calculate λ_κ
12 **for** $j = 1$ to φ
13 **if** $\lambda_j \geq j$ **then** $\Lambda_j = \Lambda_j \cup s_\kappa$
14 **if** $\Upsilon(\vec{w}_i, \vec{w}_{s_\kappa,i}) = 1$ **then** $\Omega = \Omega \cup s_\kappa$
15 **if** $\mathcal{L}[s_\kappa] > \psi$ **then** $\mathcal{B} = \mathcal{B} \cup s_\kappa$
16 **for** $j = 0$ to $\chi - 1$
17 $D_{j-1} = D_j$
18 $D_\chi = \{\vec{w}_{s_1,i}, \ldots, \vec{w}_{s_d,i}\}$
19 **else**
20 $t = 0$
21 $\mathcal{L}[s_j] = 0, j = 1, \ldots, N$

Fig. 4. On-line step of the EDD scheme.

B. The Storage-Efficient EDD (SEDD) Scheme

It can be observed from EDD that each node should maintain a list $\mathcal{L}$, leading to $O(n)$ storage overhead. Here, a storage-efficient EDD (SEDD) scheme is proposed based on the tradeoff between storage overhead and time interval's length.

The basic idea behind SEDD is that instead of monitoring all nodes, each node only monitors a subset of nodes, called *monitor set*, in a specific time interval. When the cardinality of the monitor set is selected as ξ, the simplest way for each node to select the nodes to be monitor at the beginning of a time interval is to randomly pick ξ distinct IDs from $\{1, \ldots, n\}$. Since the storage overhead is equal to the number of nodes being monitored, the storage overhead is reduced to the cardinality of the monitor set, $O(\xi)$, in the SEDD scheme.

C. Calculating μ_1, μ_2, σ_1^2, and σ_2^2

The assumptions required to calculate μ_1, μ_2, σ_1^2, and σ_2^2 are considered and stated as follows. We consider a simplified random waypoint model in which, at the beginning, n nodes are distributed uniformly in the sensing region of size $s \times s$. At step i, each node moves from the current position P_{i-1} to a randomly selected destination point (waypoint) P_i with a constant velocity v. After reaching P_i, each pauses for a constant time w to communicate with neighboring nodes. On the transition from a waypoint to the next waypoint, the node does not communicate with the other nodes. Let *communication disk* be the communication region formed by a sensor node with communication range r. We assume that each communication disk is entirely inside the sensing region for simplicity.

Assume that the node u takes τ steps during a certain time interval. Let the length of i-th step be ℓ_i. The time taken by the i-th step is $t_i = \ell_i/v + w$. We can derive that $E[t_i] = E[\frac{\ell_i}{v} + w] = \frac{E[\ell_i]}{v} + w$ and $E[t_i^2] = E[(\frac{\ell_i}{v} + w)^2] = \frac{E[\ell_i^2]}{v^2} + \frac{2w}{v}E[\ell_i] + w^2$. Accordingly, the variance of t_i can be derived as:

$$Var[t_i^2] = \frac{E[\ell_i^2]}{v^2} + \frac{2w}{v}E[\ell_i] + w^2 - (\frac{E[\ell_i]}{v} + w)^2. \quad (1)$$

We know from [2] that, if the sensing field is a square region with size $s \times s$, then $E[\ell_i] = 0.5214s$ and $E[\ell_i^2] = \frac{s^2}{3}$. The number of steps, $\tau(T)$, taken by the node m within the time interval T can be defined as:

$$\tau(T) = \max\{k : S_k \leq T\}, \text{ where } S_k = \sum_{i=1}^{k} t_i. \quad (2)$$

Since the random variables t_i are independent and identically-distributed, $\tau(T)$ can be formulated as a renewal process [12]. Let F_k be the cumulative distribution function of S_k. From the theory of the renewal process [12], we can know that $Pr[\tau(T) = k] = F_k(T) - F_{k+1}(T)$. Since the sensing field we consider is a $s \times s$ square region, the length of the longest path is $\sqrt{2}s$. Therefore, we have $\tau \geq \tau_{\min} = \frac{T}{\sqrt{2}s/v+w}$. On the other hand, by considering the case that the node stays the current position every step, we have $\tau \leq \tau_{\max} = T/w$. At each step, the node u is located within the communication

disk with the probability $p = \pi r^2/s^2$. Let δ be the number of times the node u is located within the communication disk during a time interval. Let Δ_h be the event that $\delta = h$ for some h. Let ϖ be the event that the node u takes τ steps during the time interval T. Thus, we can know

$$Pr[\Delta_h|\varpi] = \binom{\tau}{h} p^h (1-p)^{\tau-h}, \tag{3}$$

and

$$Pr[\Delta_h] = \sum_{\tau=\tau_{\min}}^{\tau_{\max}} \binom{\tau}{h} p^h (1-p)^{\tau-h} Pr[\tau], \tag{4}$$

$$= \sum_{\tau=\tau_{\min}}^{\tau_{\max}} \binom{\tau}{h} p^h (1-p)^{\tau-h} (Pr[S_\tau \leq T] - Pr[S_{\tau+1} \leq T]). \tag{5}$$

Since Central Limit Theorem (CLT) can be applied on S_k to approximate S_k with a normal distribution, where

$$E[S_k] = kE[t_i] \text{ and } Var[S_k] = kVar[t_i], \tag{6}$$

$Pr[S_\tau \leq T]$ and $Pr[S_{\tau+1} \leq T]$ can be calculated from Gaussian approximation for S_τ and $S_{\tau+1}$. Since the pdf of δ, $Pr[\Delta_h]$, can be known exactly from the Eq. (5), the parameters μ_1 and σ_1^2 can be obtained by assuming one single communication disk in the sensing field. Similarly, the parameters μ_2 and σ_2^2 can be calculated by placing two or more communication disks in the sensing field.

IV. Security and Performance Evaluation

Security. A possible strategy, called *selected silence*, which can be adopted by the replicas is to selectively broadcast the beacon so that the threshold ψ will not be reached. In cases where two replicas are considered, selected silence can be accomplished by either broadcasting the beacon every two moves or stopping broadcasting if the replicas are aware of the fact that the threshold ψ is almost reached. A common characteristic existing among various realizations of selected silence is that the replicas do not broadcast the beacon per move. Thus, this observation can be utilized to detect the replicas adopting selected silence. For example, consider the case that the node u receives the beacon $b_{v,i}$ from the node v at the time t_i and knows that they will still be the neighbor of each other from the information carried in $\vec{w}_{v,i}$ and $\vec{w}_{u,i}$. If u does not receive the beacon at the time t_{i+1}, then v will be the replicas (lines $5 \sim 6$ in Fig. 4). On the contrary, consider the case that u receives the beacon b_v from v at the time t_i and knows that they will not be the neighbor of each other at the current time from the information carried in $\vec{w}_{v,i}$ and $\vec{w}_{u,i}$ If u receives the beacon at the time t_{i+1}, then v will be the replicas (lines $7 \sim 8$ in Fig. 4). It should be noted that line 9, and lines $11 \sim 18$ are used to prepare the necessary materials for supporting the verifications mentioned above in order to prevent malicious revocation message made by replicas. However, due to limited space, the details are omitted here.

Detection Time. When the replicas are placed into the network at a certain time interval T_i, they can be detected at the time interval T_{i+1} with high probability. In other words, if the replicas exist, at most $2T$ time units are required to finish detection. In case the replicas utilize the selective silence, only one genuine node finding such replicas can flood the revocation message to the network. Thus, the replicas adopting selective silence will be revoked almost immediately.

Storage Overhead. The storage overhead for the EDD scheme is $O(n)$ due to the list $\mathcal{L}$. It appears that EDD is inapplicable to the sensor networks. However, EDD is found to be applicable for current mobile sensor networks according to the following observations: 1) Compared with the inherent characteristics of sensor nodes such as limited communication capability and battery power, the limited storage can be properly relaxed by either attaching memory module to the sensor node or exploiting advanced sensor nodes [7], [13], [15]. 2) The current sensor networks [7], [13], [15] usually consist of tens of sensor nodes. In other words, the scale is not large and each element in the list $\mathcal{L}$ only needs several bits in practice so that the storage overhead $O(n)$ is affordable for the current sensor nodes. If the sensor nodes with extremely scarce resource are considered or the scale of the network is relatively large, then the EDD scheme might be inapplicable for the sensor nodes. However, the SEDD scheme can tradeoff the storage overhead and the detection time, and achieve only $O(\xi)$ storage overhead without compromising the other characteristics of the EDD scheme.

Computation Overhead. The off-line step of EDD may be a time-consuming task. However, it is executed, prior to the sensor deployment, by the network planner instead of the sensor node. In addition, since the network planner usually at least has PC-level computation power, this task can be successfully accomplished. As to the computation overhead of sensor nodes, in addition to the operations required for the signed messages, only simple arithmetic operations such as addition and set operations such as intersection are required to be performed, which are affordable for the current generation sensor nodes.

Communication Overhead. It is known that communication dominates the energy consumption of a sensor node. Hence, to reduce the energy consumption of networks, it should emphasis on reducing communication overhead. In both the EDD and SEDD schemes, each node u listens the beacon $b_{v,i} = (v, \vec{w}_v, t_i)$ broadcasted by its neighbor v. Upon receiving the beacon, the node u checks if v is a replica by executing the on-line step of EDD. It can be observed that the additional communication overhead incurred by the EDD and SEDD schemes is only b_v, resulting in $O(1)$ communication overhead in general case. Even better, when certain applications such as tracking are considered, since the periodical broadcast of beacon has been required in such an application, the communication overhead could become zero by piggybacking $\vec{w}_{v,i}$ in the broadcasted message. The comparison for replica detection schemes in terms of the detection type and the communication cost is shown in Table I. Note that one special case is the network with replicas adopting selective silence, which can be discovered and revoked by flooding revocation messages with $O(n)$ communication overhead. However, we argue that this is a rare case because the replicas adopting selective silence will be revoked almost immediately so that

TABLE I
COMPARISON OF THE NODE REPLICA DETECTION SCHEMES IN TERMS OF THE DETECTION TYPE AND COMMUNICATION COST.

Schemes	Type	Comm. Cost
RKP [1]	Centralized	$O(n \log n)$
SET [5]	Centralized	$O(n)$
Ho *et al.* [9]	Centralized	$O(\sqrt{n})$
Xing *et al.* [14]	Centralized	$O(\sqrt{n})$
RED [3]	Distributed	$O(n\sqrt{n})$
Broadcast, DM, RM, LSM [11]	Distributed	$O(n^2)$
XED [17]	Distributed	$O(1)$
SDC, P-MPC [18]	Distributed	$O(n\sqrt{n})$
EDD and SEDD (this paper)	Distributed	$O(1)$/$O(n)$

replicas rarely use selective silence.

V. SIMULATION RESULT

Due to limited space, only the simulation results of EDD, which are shown in Fig. 5, are provided. It shows that the genuine nodes and replicas can be distinguished well by properly setting ψ. For example, Fig. 5(d) shows that in a interval consisting of 12000 moves the number of times a genuine node encounters another genuine node is highly unlikely over 85. On the other hand, if the replicas are forced to broadcast beacon regularly, the number of times a genuine node encounters the replicas is highly likely over 85. With such consideration, if ψ is set to be 85, the genuine nodes and replicas can be almost perfectly distinguished.

There are many factors affecting the efficiency and effectiveness of the proposed schemes. Two of them are the communication range of sensor nodes and the length of time interval. It can be observed from Fig. 5 that it is easier to distinguish the replicas from the genuine nodes in the network composed of sensor nodes with large communication range than that with short communication range. The reason is that the replica with more than one duplicate is easier to be the neighbor of a node, leading to rapid increase of the number of encounters. On the other hand, it can be observed from Fig. 5 that it is easier to distinguish the replicas from the genuine nodes if larger time interval is used. This is because from the viewpoint of law of large numbers, the number of encounters for replicas is twice greater than that for genuine nodes in a long-term period.

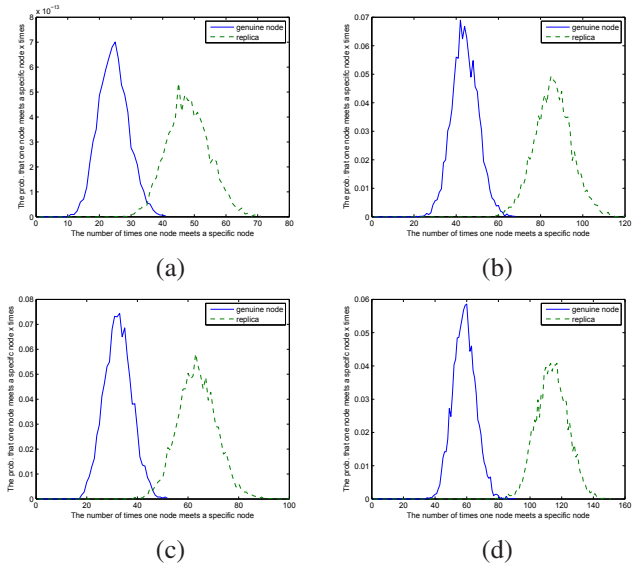


Fig. 5. Detection of node replicas in the EDD scheme: (a) 9000 moves/0 and 2 replicas/comm. range is 30; (b) 9000 moves/0 and 2 replicas/comm. range is 50; (c) 12000 moves/0 and 2 replicas/comm. range is 30; (d) 12000 moves/0 and 2 replicas/comm. range is 50.

VI. CONCLUSION

In this paper, we propose two schemes, EDD and SEDD, for defending against node replication attacks in mobile sensor networks. Our methods are effective and efficient in terms of the communication/computation/storage overheads.

Acknowledgment: Chia-Mu Yu and Chun-Shien Lu were supported by NSC 97-2221-E-001-008. Sy-Yen Kuo was supported by NSC 96-2628-E-002-138-MY3.

REFERENCES

[1] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the Detection of Clones in Sensor Networks Using Random Key Predistribution," *IEEE Transactions on Systems, Man, and Cybernetics - Part C: Applications and Reviews*, vol. 37, no. 6, pp. 1246-1258, Nov. 2007.

[2] C. Bettstetter, H. Hartenstein, and X. P. Costa. Stochastic Properties of the Random Waypoint Mobility Model. *Wireless Networks*, vol. 10, no. 5, pp. 555-567, 2004.

[3] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks." *ACM MobiHoc*, 2007.

[4] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei. Emergent properties: detection of the node-capture attack in mobile wireless sensor networks. In *ACM WiSec*, 2008.

[5] H. Choi, S. Zhu, T. F. La Porta, "SET: Detecting node clones in Sensor Networks," *IEEE/ICST Securecomm*, 2007.

[6] L. Eschenauer and V. Gligor, "A Key-management Scheme for Distributed sensor networks," *ACM CCS*, 2002.

[7] B. Hull, V. Bychkovskiy, K. Chen, M. Goraczko, E. Shih, Y. Zhang, H. Balakrishnan, and S. Madden. CarTel: A Distributed Mobile Sensor Computing System. In *ACM SenSys*, 2006.

[8] L. Hu and D. Evans. Localization for mobile sensor networks. In *ACM MobiCom*, 2004.

[9] J. Ho, M. Wright, and S. K. Das. Fast Detection of Node Replication Attacks in Mobile Sensor Networks, In *IEEE ICNP*, 2008. (poster)

[10] D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. *Mobile Computing*, pp. 153-181, 1996.

[11] B. Parno, A. Perrig, and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks,", *IEEE S&P*, 2005.

[12] S. M. Ross. Introduction to Probability Models. Academic Press, 2006.

[13] P. Volgyesi, G. Balogh, A. Nadas, C. B. Nash, and A. Ledeczi. Shooter Localization and Weapon Classification with Soldier-Wearable Networked Sensors. In *ACM MobiSys*, 2007.

[14] K. Xing, F. Liu, X. Cheng, and D. Du. Real Time Detection of Clone Attack in Wireless Sensor Networks, In *IEEE ICDCS*, 2008.

[15] T. Ya, D. Ganesan, and R. Manmatha. Distributed Image Search in Sensor Networks. In *ACM SenSys*, 2008.

[16] J. Yi, J. Koo, and H. Cha. A Localization Technique for Mobile Sensor Networks Using Archived Anchor Information. In *IEEE SECON*, 2008.

[17] C.-M. Yu, C.-S. Lu, S.-Y. Kuo. Mobile Sensor Network Resilient Against Node Replication Attacks. In *IEEE SECON*, 2008. (poster)

[18] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks," *ACSAC*, 2007.

[19] L. Zhou, J. Ni, and C. V. Ravishankar. Supporting Secure Communication and Data Collection in Mobile Sensor Networks. In *IEEE INFOCOM*, 2006.