ISSN:0975-9646

Detection of Node Replication Attacks in Mobile Sensor Networks Using Localized Algorithms

Pooja Chaturvedi, Shyam S. Gupta

Computer Department, Pune University
Pune, India

***Abstract*— Node replication detection is a challenging problem. Though the defending against node replication attacks demands immediate attention as compared to the extensive exploration on the defense against node replication attacks in static networks, only a few solutions in mobile networks have been presented. Additionally, whereas most of the presented schemes in static networks exist on the witness-finding strategy that cannot be applied to mobile networks, the velocity-exceeding strategy used in existing schemes in mobile networks incurs efficiency and security problems. Thus, based on our devised challenge-and-response and encounter-number approaches, required algorithms are proposed to resist node replication attacks in mobile sensor networks. The advantages of our proposed algorithms include 1) localized detection; 2) efficiency and effectiveness; 3) network-wide synchronization avoidance; and 4) network-wide revocation avoidance. The Performance comparisons with existing methods are provided to demonstrate the efficiency of our proposed algorithms. Prototype implementation on TelosB mote demonstrates the practicality of our proposed methods.**

***Keywords*— Attack, security, wireless sensor networks.**

I. INTRODUCTION

Sensor networks consist of a number of sensor nodes with limited resources, which is useful to applications, like environment monitoring and object tracking. To perform critical operations sensor networks could be deployed in a region which is known as hostile region. Due to a situation occurs where the adversary can compromise one sensor node, fabricate many replicas having the same identity (ID) from the captured Node, and place these replicas back into strategic positions in the network for further malicious activities. So this is also called as *node replication attack*. With the security point of view, the attack of node replication is absolutely harmful to networks because replicas, having keys, can easily launch insider attacks, without easily being detected. Although the problem of node replication detection in static networks has been extensively studied, only a few schemes have been proposed for mobile sensor networks. Although the problem of node replication detection in static networks has been extensively studied, only a few schemes have been proposed for mobile sensor networks.

With the consideration of nodes.' mobility and the distributed nature of sensor networks, it is desirable, but very challenging, to have efficient and effective distributed algorithms for detecting replicas in mobile sensor networks. Although the problem of node replication detection in static networks has been extensively studied, only a few schemes have been proposed for mobile sensor networks.

RELATED CONCEPTS:

According to assumption that a sensor node, when attempting to join the network, must broadcast a signed location claim to its neighbours, most of the existing distributed detection protocols [1], [2], [5] adopt the witness-finding strategy to detect the replicas.

When there are replicas in the network, the witnesses, according to the received location claims, have possibility to find a node ID with two distant locations, which implies that the node ID is being used by replicas. Afterward, the detected replicas can be excluded using, for example, network-wide revocation. The detection algorithms proposed in [1], [2], [4], [5]–[7] all belong to this category. For example, RM and LSM were proposed in [2] to determine the witnesses randomly. The difference between RM and LSM is that the witness nodes that find the conflicting location in the former are primarily affected by the number of witness nodes and the ones in the latter are prima affected by the forwarding traces of location claims. SDC and P-MPC [5] can be thought of as the cell versions of RM and LSM.

In particular, before sensor deployment, the sensing region is divided into cells. Compared to RM and LSM, which forward location claims node by node, SDC and P-MPC forward location claims cell by cell. Based on the assumption that the special centralized broadcasting devices, such as satellites and Unmanned Aerial Vehicles (UAVs), help broadcast a pseudorandom number to all of the sensor nodes periodically, RED [1] also adopts the concept of witness-finding to detect node replication attacks but with lower communication cost. The efficiency and effectiveness of RED can also be confirmed in [8]. Based on the double ruling [4], a suite of memory-efficient detection

Algorithm is introduced in [7]. The idea is to guarantee the intersection of traces in LSM via double ruling and to reduce the memory usage of intermediate nodes in LSM via the Bloom filter. In addition, to better distribute the responsibility of witness node selection, the random walk technique is utilized in LSM in [6].

Previously, Conti et al. [9] propose a distributed algorithm for replica detection in the two-dimensional mobility model. Note that in the two dimensional mobility model, the nodes are uniformly and randomly placed in the network at the beginning of each round. One of useful

characteristics is that the position of each node is independent of the one in the previous round. By doing so, each node is able to check whether there is a node appearing in two distant locations at the same time. Each node in [9] keeps a list of node IDs, time, and the locations it encountered in the past time units. Each node then broadcasts the above information to its neighbouring nodes per move.

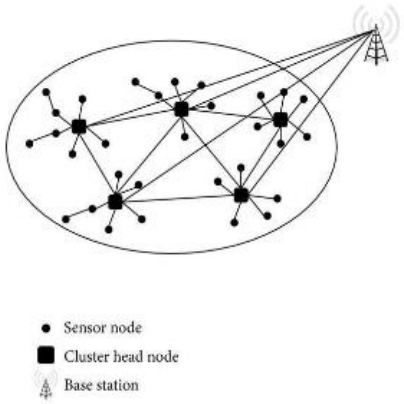

Fig. 1 Hierarchical sensor network architecture.

In Mobile Environments Detecting Replicas have Various Challenges, these are as follows:

The witness-finding strategy can adapt to mobile environments if a timestamp is associated with each location claim. In addition, setting a fixed time window t in advance and performing the witness- finding strategy for every t units of time can also keep witness- finding feasible in mobile sensor networks. Therefore, accurate time synchronization among all the nodes in the network is necessary. Additionally, when witness-finding is applied to mobile sensor networks, routing the message to the witnesses incurs even higher communication cost. After completion of the replica identifications, a message used to revoke the replicas, possibly issued by the origin station or the witness that detects the replicas, is usually flooded throughout the network. Therefore, network-wide broadcast is highly energy-consuming and, hence in the protocol design, it should be avoided.

Hence, the witness nodes cannot discover the existence of replicas. To cope with this issue, localized algorithms could enhance the resilience against node compromise. In spite of the effectiveness in detecting replicas, all of the schemes adopting witness-finding
have the common drawback that the detection period cannot be determined. In other words, the replica detection algorithm can be triggered to identify the replicas only after the network anomaly has been noticed by the network planner. Therefore, a detection algorithm that can always automatically detect the replica is desirable.

Since in the existing system, we have found some difficulties that will be avoided in the proposed system. So, at first, the network and security models used in this paper are presented. Also, the proposed XED and EDD schemes will be presented. At last, the conclusion will be made.

II. LITERATURE SURVEY

Wireless sensor networks are often deployed in hostile environments, where an adversary can physically capture some of the nodes. Once a node is captured, the attacker can re-program it and replicate the node in a large number of clones, thus easily taking over the network. The detection of node replication attacks in a wireless sensor network is therefore a fundamental problem. A few distributed solutions have recently been proposed. However, these solutions are not satisfactory. First, they are energy and memory demanding: A serious drawback for any protocol that is to be used in resource constrained environment such as a sensor network. Further, they are vulnerable to specific adversary models introduced in this paper. The contributions of this work are threefold. First, we analyse the desirable properties of a distributed mechanism for the detection of node replication attacks. Second, we show that the known solutions for this problem do not completely meet our requirements. Third, we propose a new Randomized, efficient, and Distributed (RED) protocol for the detection of node replication attacks and we show that it is completely satisfactory with respect to the requirements. Extensive simulations also show that our protocol is highly efficient in communication, memory, and computation, that it sets out an improved attack detection probability compared to the best solutions in the literature, and that it is resistant to the new kind of attacks we introduce in this paper, while other solutions are not.

Wireless Sensor Networks (WSNs) are often deployed in hostile environments where an adversary can physically capture some of the nodes, first can reprogram, and then, can replicate them in a large number of clones, easily taking control over the network. A few distributed solutions to address this fundamental problem have been recently proposed. However, these solutions are not satisfactory. First, they are energy and memory demanding: A serious drawback for any protocol to be used in the WSN-resource-constrained environment. Further, they are vulnerable to the specific adversary models introduced in this paper. The contributions of this work are threefold. First, we analyze the desirable properties of a distributed mechanism for the detection of node replication attacks. Second, we show that the known solutions for this problem do not completely meet our requirements. Third, we propose a new self-healing, Randomized, Efficient, and Distributed (RED) protocol for the detection of node replication attacks, and we show that it satisfies the introduced requirements. Finally, extensive simulations show that our protocol is highly efficient in communication, memory, and computation; is much more effective than competing solutions in the literature; and is resistant to the new kind of attacks introduced in this paper, while other solutions are not.

III. NETWORK MODEL

In this paper, we assume that there are only stationary sensor nodes in the wireless sensor network. We also assume that the communications between the stationary

sensor nodes are bi-directional, which is also an assumption of most of previous detection schemes.

Stationary nodes can get their geographic location by using positioning device (e.g., GPS device) or positioning algorithms [15–18]. Also, we assume that all the sensor nodes are loosely time synchronized using time synchronization techniques .the sensor network consists of n sensor nodes with IDs, (1 ……. n). The communication is assumed to be symmetric. Additionally, each node is assumed to periodically broadcast a beacon containing its ID to its neighbours. This is usually same length. None the less, the
relies on the assumption that the replicas do not collude with each other. When replicas can communicate with each other, the replica can always share the newest received random numbers with the other neighbouring replicas, thus degrading the detection capability because multiple replicas are able to reply with the correct random number to encountered genuine nodes accordingly time among sensor nodes does not need to be synchronized. The sensor nodes have mobility and move according to the Random Way Point (RWP) model [12], which is commonly used in modelling the mobility of ad hoc and sensor networks [13]. Each node is assumed to be able to be aware of its geographic position. In this model, each node randomly chooses a destination point known as waypoint in the sensing field, and moves toward it with velocity, randomly selected from a predefined interval. After reaching the destination point, the node remains static for a random time and then starts moving again according to the same rule. To simplify the analysis, we assume each node has neighbours on average per move. Finally, we follow the conventional assumption in prior works that the network utilizes an identity-based public key system [10], [11], so signature generation and verification are feasible. In general, the models used in this paper are the same as the ones in prior works.

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 compromised. Sensor nodes could be compromised by the adversary immediately after sensor deployment. The adversary has all of the legitimate credentials from the compromised nodes. After that, the adversary deploys two or more nodes with the same ID; i.e., replicas, into the network. Replicas can communicate and collude with each other in order to avoid replica detection in EDD For example; replicas can share their credentials and can selectively be silent for a certain time if required after the collusion. Owing to the use of the digital signature function [10], [11], the replicas cannot create a new ID or disguise themselves as the nodes being not compromised before, because it is too difficult for the adversary to have the corresponding security credentials. Since the focus of this paper is on the node replication attack, despite many security issues on sensor networks such as key management, replay attack , wormhole attack , Sybil attack , secure query, etc., can be handled in our proposed work.

Algorithm: XED-On-line-step

Here u = node and t=time
//$V=v_1,\ldots, v_d$ is the neighbours of u
//$\{v_1,\ldots v_d\} \notin \beta^{(u)}$
1: send $L_v^{(u)}[v_1],\ldots, L_v^{(u)}[v_d]$ to $v_1,\ldots v_d$, respectively
2: Receive $L_v^{(v1)}[u],\ldots,$ receive $L_v^{(vd)}[u]$

3: for k=1 to d
4: If $h(L_s^{(u)}[v_k]) == (L_v^{(vk)}[u]$
5: **select** $\alpha \in [1, 2^{\sigma}- 1]$ and set $L_s^{(u)}[v_k]= \alpha$
6: calculate h(α) then send h(α) to v_k
7: otherwise
8: set$\beta^{(u)}] = \beta^{(u)} \cup \{ v_k \}$

Fig. 2. Online step of the XED scheme.

XED:

The idea behind XED is motivated by the observation that, if a sensor node u meets another sensor node v at an earlier time and u sends a random number to v at that time, then, when u and v meet again, u can ascertain whether this is the node u met before by requesting the random number. Note that, in XED, we assume that the replicas cannot collude with each other but this assumption will be removed in our next solution in. In addition, all of the exchanged messages should be signed unless specifically noted. Moreover, the XED scheme is composed of two steps: an offline step and an online step. The former is executed before sensor deployment while the latter is executed by each node after deployment. The effectiveness of XED, unfortunately, heavily

EDD:

The main idea behind EDD is motivated by the following observations. The maximum number of times, Y1, that node u encounters a specific node v, should be limited with high probability during a fixed period of time, while the minimum number of times, Y2, that u encounters the replicas with the same ID v, and should be larger than a threshold during the same period of time. According to these observations, if each node can discriminate between these two cases, it has the ability to identify the replicas. Different from XED, EDD assumes that the replicas can collude with each other. In addition, all of the exchanged messages should be signed unless specifically noted. Particularly, the EDD scheme is composed of two steps: an offline step an and an online step. The offline step is performed before 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 online step will be performed by each node at each move. Each node checks whether the encountered nodes are replicas by comparing ψ with the corresponding number of encounters. In the following, we somewhat abuse the notation; we denote the start time of each interval as t0.

The Offline and Online scheme of EDD Shown below:

Algorithm-: EDD –Off –line –step

1: set T = 1 and $\beta^{(u)} = \phi$, $u \in [1, n]$

2: set $L^{(u)}[i] = 0,1 \leq i \leq n, u \in [1,n]$

3: do

4: Set T= T+1

5: Find $\mu 1$, $\mu 2$, σ_1^2 and σ_2^2

6: Where Y1= $\mu 1 + 3\sigma_1$ and Y2 = = $\mu 2 + 3\sigma_2$

7: if Y1 < Y2

8: $Take\ \varphi = \frac{Y2-Y1}{2}$

Fig. 3. Offline step of the EDD scheme.

Algorithm: EDD_Oline Step

// algorithm is used by node *u* at each time *t*

//where $v_1, \ldots, v_d$ are the neighbors of *u*

//all neighbor V={$v_1, \ldots v_d$} $\notin \beta^{(u)}$

1: broadcast beacon b_u // b_u= (*u*) contains the ID of *u*

2. If t $\neq t_0$

3. Receive beacon $b_{v1}, \ldots b_{vd}$

4. For *k*= 1 to d

5: $L^{(u)}[v_k] = L^{(u)}[v_k] + 1$

6: $L^{(u)}[v_k] > \varphi$ then set $\beta^{(u)} = \beta^{(u)} \cup \{v_k\}$

7: otherwise *t=t0*

8: set $L^{(u)}[s_k] = 0, k = 1, \ldots, n$

Fig. 4 Online step of the EDD scheme.

III. Proposed Approach

Problem Definition:

As sensor networks could be deployed in a hostile region to perform critical missions, the sensor networks are unattended and the sensor nodes normally are not equipped with tamper-resistant hardware. The replicas can be considered as legitimate members of the network, making detection difficult. From the security point of view, the node replication attack is extremely harmful to networks. Hence as result of this, a scenario occurs where the adversary can compromise one sensor node, fabricate many replicas having the same identity (ID) from the captured node, and place these replicas back into strategic positions in the network for further malicious activities. This is a so-called node replication attack. Although the problem of node replication detection in static networks has been extensively studied, only a few schemes have been proposed for mobile sensor networks. Even worse, as indicated in [14], the techniques used in detecting replicas in static environments are not useful in identifying replicas in mobile environments.

Proposed Work:

We propose a novel approach named the L-EDD algorithm was proposed. The algorithm has properties which make it suitable for handling streaming traffic in tactical network. The simulation results for two serviced classes show that L-EDD algorithm allows differentiation of loss ratio among classes. The differentiation is relative which means that improvement of performance for one class implies degradation of another one. Simulation tests were performed for two types of traffic, Poisson and CBR. Additionally, simulation results proved that there is a possibility to create a privileged class, with stringent requirements concerning delay and losses.

L-EDD Algorithm:

The L-EDD algorithm is an enhancement of EDD algorithm to support differentiation of delay and losses. It uses similar mechanism as in Round Robin algorithm to choose next packet/cell to service. We expect that such modified EDD scheduler will better treat good behaving flows in present of overload.

To decrease complexity of algorithm we did not apply the sorted queue. L-EDD algorithm uses multiple FIFO system to serve flows with different deadlines T_D. Using of such a system allows aggregation of flows into classes according to their deadlines. We assume that the range of deadline values is limited. Deadlines assigned to cells are not continuous set of values, but belong to defined, finite subset D={d_1; d_2; …; d_n), where n is the number of classes. Next, such classified traffic is served by multiple FIFO system, where a single FIFO queue is assigned for each of class. The main assumption for L-EDD is that for each class (FIFO buffer) a **limit counter LC** is assigned.

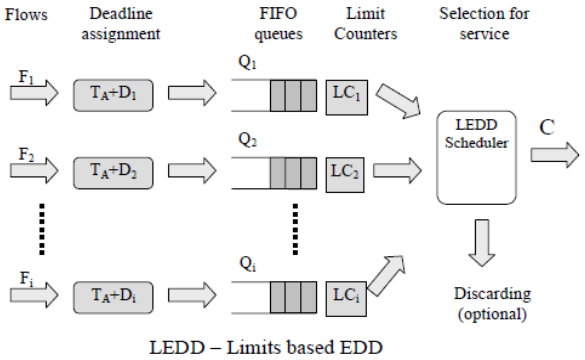

Fig.5. The proposed L-EDD algorithm – deadline and limit based EDD scheduling.

There were three tests provided to investigate behavior of proposed algorithm. The first and second test compared abilities of Classic EDD and L-EDD algorithms for providing delay and losses differentiation respectively. The second test examined handling of CBR traffic in the presence of congestion caused by traffic with Poisson characteristics.

Incoming traffic was Poisson distributed in the first two tests. The third test was performed using CBR sources with Poisson traffic in the background. Results of simulation were obtained during simulated time interval, which provided at least several millions of events.

IV Conclusion And Future Work.

In this paper, apart from two replica detection algorithms for mobile sensor networks, XED and EDD, we proposed the L-EDD algorithm. The algorithm has properties which make it suitable for handling streaming traffic in a mobile sensor network. The simulation results for two serviced classes which show that L-EDD algorithm allows differentiation of loss ratio among classes. The differentiation is relative which means that improvement of performance for one class implies degradation of another one. Simulation tests were performed for two types of traffic, Poisson and CBR.

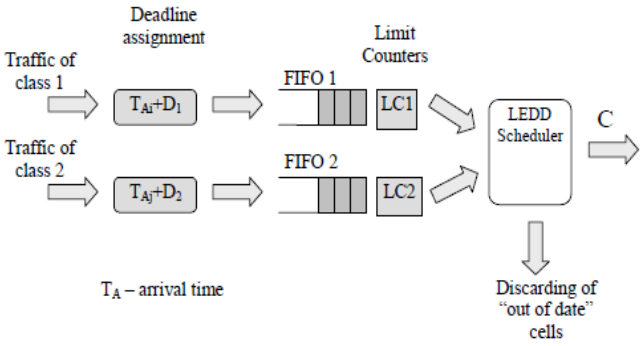

Fig.6. Functional diagram of implemented L-EDD simulator.

REFERENCES

[1] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, ."A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks,." in *Proc. ACMInt. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc)*, Montreal, Canada, 2007,pp. 80.–89.

[2] B. Parno, A. Perrig, and V. Gligor, ."Distributed detection of node replication attacks in sensor networks,." in *Proc. IEEE Symp. Security and Privacy (S&P)*, Oakland, CA, USA, 2005, pp. 49.–63.

[3] G. Sharma and R. Mazumdar, ."Scaling laws for capacity and delay in wireless ad hoc networks with random mobility,." in *Proc. IEEE Int. Conf. Communications (ICC)*, Paris, France, 2004, pp. 3869. 3873.

[4] R. Sarkar, X. Zhu, and J. Gao, ."Double rulings for information brokerage in sensor networks,." *IEEE/ACM Trans. Netw.*, vol. 17, no. 6, pp. 1902.–1915, Dec. 2009.

[5] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, ."Localized multicast: Efficient and distributed replica detection in large-scale sensor networks,." *IEEE Trans. Mobile Comput.*, vol. 9, no. 7, pp. 913.–926, Jul. 2010.

[6] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, ."Random-walk based approach to detect clone attacks in wireless sensor networks,." *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 677.–691, Jun. 2010.

[7] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, ."Memory efficient protocols for detecting node replication attacks in wireless sensor networks, ." in *Proc. IEEE Int. Conf. Network Protocols(ICNP)*,Princeton, NJ, USA, 2009, pp. 284.–293.

[8] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, ."Distributed detection of clone attacks in wireless sensor networks,." *IEEE Trans. Depend. Secure Comput.*, vol. 8, no. 5, pp. 685.–698, Sep./Oct. 2012.

[9] M. Conti, R. D. Pietro, and A. Spognardi, ."Wireless sensor replica detection in mobile environment,." in *Proc. Int. Conf. Distributed Computing and Networking (ICDCN)*, Hong Kong, China, 2012, pp. 249.–264.

[10] A. Liu and P. Ning, ."TinyECC: A con□gurable library for elliptic curve cryptography in wireless sensor networks,." in *Proc. Int. Conf. Information Processing in Sensor Networks (IPSN)*, Missouri, USA, 2008, pp. 245.–256.

[11] D. J. Malan, M. Welsh, and M. D. Smith, ."Implementing public-key infrastructure for sensor networks,." *ACM Trans. Sensor Network*, vol. 4, no. 4, pp. 1.–23, 2008.

[12] D. B. Johnson and D. A. Maltz, ."Dynamic source routing in ad hoc wireless networks,." *Mobile Comput.*, pp. 153.–181, 1996.

[13] J. Yi, J. Koo, and H. Cha, ."A localization technique for mobile sensor networks using archived anchor information,." in *Proc. IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON)*, California, USA, 2008, pp. 64.–72.

[14] K. Xing and X. Cheng, ."From time domain to space domain: Detecting replica attacks in mobile ad hoc networks,." in *Proc. IEEE Int. Conf. Computer Communications (INFOCOM)*, San Diego, CA, USA, 2010, pp. 1.–9.