A Secure Distributed Detection of Node Replication Attacks in Mobile WSN using Localized Algorithms

R.Harikrishnan, S.Narendran

Abstract— 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. This allows a situation where the adversary can compromise one sensor node, fabricate many replicas having the same identity 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. Since the credentials of replicas are all clones of the captured nodes, the replicas can be considered as legitimate members of the network, making detection difficult. Based on the assumption that a sensor node, when attempting to join the network, must broadcast a signed location claim to its neighbors, most of the existing distributed detection protocols adopt the witness-finding strategy to detect the replicas. In particular, the general procedure of applying witness-finding to detect the replicas can be stated as follows. After collecting the signed location claims for each neighbor of the node , where and denote the location of and the digital signature function respectively, sends the collected signed location claims to a properly selected subset of nodes, which are witnesses. 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, network-wide revocation.

Index Terms— attack, claim node, identity, replication, sensor node, witness node, wireless sensor networks.

1 INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. Sensor nodes operate in hostile environment such as battle fields and surveillance zones. Due to their operating nature, WSNs are of unattended, hence prone to several kinds of novel attacks. The mission-critical nature of sensor network applications implies that any compromise or loss of sensory resource due to a malicious attack launched by the adversary-class can cause significant damage to the entire network. Static WSN contains more number of sensor nodes in it, for sense data from environment, those are situated as stable position in the network, they don't move anywhere inside the network. Mobile WSN has little different from Static WSN, it also contains more number of nodes in it, but those nodes are always in moving inside the network for sense data. We can classify sensor network attacks into three main categories: Identity Attacks, Routing Attacks & Network Intrusion. Identity attacks intend to steal the identities of legitimate nodes operating in the sensor network. The identity attacks are classified as Sybil attacks and Clone (Replication) attacks. In Sybil attack, the WSN is subverted by a malicious node which forges large identities in number of fake order to disrupt the network's protocols. Principally, a node replication attack in WSN is an attempt by the adversary to add one or more nodes to the network that use the same ID as another node in the network.

An identity attack called replication attack where one or more nodes illegitimately claim an identity of legitimate node and replicated in whole WSN. The detection of node replication attacks in a wireless sensor network is therefore a fundamental problem.

2 IMPLICATION OF REPLICATION ATTACK

2.1 Goals

For a given sensor network, we assume that sensor node not tamper proof and deployed in unattended location. The adversary can capture the node collect all the secret keys, data and code stored on it. All the credentials are exposed to the attacker. The attacker can easily replicate it in a large number of clones and deploy them on the network. We evaluate each protocol's security by examining the probability of detecting an attack given that the adversary inserts L replicas of a subverted node. . The protocol must provide robust detection even if the adversary captures additional nodes. We also evaluate the efficiency of each protocol. The Communication (for both sending and receiving) among nodes requires at least an order of magnitude power than any other operation. So our first priority to minimize the communication cost for both whole network and individual nodes (hotspots quickly exhausts power), which one

- *R.Harikrishnan is currently working as Assistant Professor in Department of Information Technology, P.B. College of Engineering in Anna University, India, PH-91-9865870701. E-mail: hari.rrec@gmail.com*
- *S.Narendran is currently pursuing master of engineering program in Computer and Communication,P.B. College of Engineering in Anna University, Country, PH-91-8903265800. E-mail: narentech21@gmail.com*

of the limitation of WSN. Another limitation is memory. Thus any protocol requiring a large amount of memory will be impractical.

2.2 Sensor Network Environments

A sensor network usually lies of hundreds, or even thousands, of small, low-cost nodes distributed over a wide area. The nodes are required to function in an unsupervised fashion even if new nodes are added, or old nodes disappear (e.g., due to power loss or accidental damage). While some networks include a central location for data collection, many operate in an entirely distributed manner, allowing the operators to retrieve aggregated data from any of the nodes in the network. Furthermore, data collection may only occur at irregular intervals. We also assume that the adversary cannot readily create new IDs for nodes. Newsome et al. describe several techniques to prevent the adversary from deploying nodes with arbitrary IDs. For example, we can tie each node's ID to the unique knowledge it possesses. If the network uses a key predistribution scheme, then a node's ID could correspond to the set of secret keys it shares with its neighbors (e.g., a node's ID is given by the hash of its secret keys). In this system, an adversary gains little advantage by claiming to possess an ID without actually holding the appropriate keys. Assuming the sensor network implements this safeguard, an adversary cannot create a new ID without guessing the appropriate keys (for most systems, this is infeasible), so instead the adversary must capture and clone a legitimate node.

3 SOLUTIONS TO REPLICATION ATTACKS AND COUNTERMEASUREMENTS

Solutions to replication attack should follow three key design goals for replica detection schemes. First, replica nodes should be detected with minimal communication, computational, and storage overheads. Second, the detection schemes should be robust and highly resilient against an attacker's attempt to break them. More specifically, the schemes should detect replicas unless the attacker compromises a substantial number of nodes. Finally, there should be no false positives, meaning that only compromised and replica nodes would be detected and revoked. This is important to prevent the attacker from turning a replica detection scheme into a tool for denial of service attacks.

Replication attack detection protocols classified as two categories of WSN: Centralized and Distributed approaches. These approaches have their own merits and demerits. The main ideas of these schemes are to have nodes report location claims that identify their positions and attempt to detect conflicting reports that signal one node in multiple locations.

3.1 Centralized Detection Approaches

In static WSN, The centralized approaches are simple, local detection (SET) and fast detection scheme with Sequential probability ratio test (SPRT) have been analysed.

In a Simple Centralized approach, the Base Station (BS) acts as centralized entity, each node sends a list of its neighbor nodes and their claimed locations to a base station. If the base station finds that there are two far distant locations for one node ID, then the node clone must have occurred. The BS simply broadcasts through the whole network to expel the cloned nodes. Then, the BS will revoke the replicated nodes.

Local Detection (SET) manages to reduce the communication cost of the preceding approach by computing set operations of exclusive subsets in the network. First, SET launches an exclusive subset maximal independent set (ESMIS) algorithm which forms exclusive unit subsets among one-hop neighbors in an only one disjointed subset which are controlled by a randomly decided leader.

Fast detection with SPRT for Mobile WSN presents SPRT has been proven to be the best mechanism in terms of the average number of observations that are required to reach a decision among all sequential and non sequential test processes. SPRT can be thought of as one dimensional random walk with lower and upper limits. the technique to detect replica attacks in mobile sensor networks. In static sensor networks, a sensor node can be considered to be replicated if it is placed at more than one location.

3.2 Distributed Detection Approaches

Distributed detection approaches can be classified broadly in to three categories in Static WSN: Node-to network Broadcasting and Witness Based strategy. And also, extremely Efficient Detection (XED) and Efficient Distributed Detection (EDD) are detection approaches in Mobile WSN.

i) Node-to network Broadcasting

This detection approach utilizes a simple broadcast protocol. Basically, each node in the network uses an authenticated broadcast message to flood the network with its location information. Each node stores the location information for its neighbors and if it receives a conflicting claim, revokes the offending node.

ii) Witness finding strategy

Most of the existing distributed detection protocols 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, to detect the replicas.

In the Random Multicast (RM), when a node broadcasts its location, each of its neighbors sends (with probability p) a digitally signed copy of the location claim to a set of randomly selected nodes. Assuming there is a replicated node, if every neighbor randomly selects $O(\sqrt{n})$ destinations, then exploiting the birthday paradox, there is a non negligible probability at least one node will receive a pair of non coherent location claims. The node that detects the existence of another node in two different locations within the same time-frame will be called witness. The RM protocol implies high communication costs: Each neighbor has to send $O(\sqrt{n})$ messages.

In the Line Selected Multicast (LSM) protocol, uses the routing topology of the network to detect replication, each node which forwards claims also saves the claim. That is, the forward-

ing nodes are also witness nodes of a node which has the node ID in a claim. Therefore, LSM gives a higher detection rate than that of RM.

SDC and P-MPC can be thought of as the cell versions of RM and LSM. Compared to RM and LSM, which forward location claims node by node, SDC and P-MPC forward location claims cell by cell.

4 Challange in Detecting Replicas in Mobile Environments

The witness-finding strategy exploits the fact that one sensor node cannot appear at different locations, but, unfortunately, the sensor nodes in mobile sensor networks have the possibility of appearing at different locations at different times, so the above schemes cannot be directly applied to mobile sensor networks. Slight modification of these schemes can be helpful for applicability to mobile sensor networks. For instance, 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. Nevertheless, accurate time synchronization among all the nodes in the network is necessary. Moreover, when witness-finding is applied to mobile sensor networks, routing the message to the witnesses. After identifying the replicas, a message used to revoke the replicas, possibly issued by the base station or the witness that detects the replicas, is usually flooded throughout the network. Nevertheless, network-wide broadcast is highly energy-consuming and, therefore, should be avoided in the protocol design.

Witness-finding could be categorized as a strategy of cooperative detection; sensor nodes collaborate in certain ways to determine which ones are the replicas. In this regard, the effectiveness of witness-finding could be reduced when a large number of sensor nodes have been compromised, because the compromised nodes can block the message issued by the nodes near the replicas. 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 the existing algorithms are built upon several other requirements, we have found that the common weakness of the existing protocols in detecting node replication attacks is that a large amount of communication cost is still unavoidable.

5 The Proposed Methods

In this section, our proposed algorithms, eXtremely Efficient Detection (XED) and Efficient Distributed Detection (EDD) for replica detection in mobile networks will be described.

5.1 Contributions

To detect the node replicas in mobile sensor networks, two localized algorithms, XED and EDD, are proposed. The techniques developed in our solutions, challenge-and-response and encounter-number, are fundamentally different from the others.

Our algorithms possess the following advantages:

• Localized Detection: XED and EDD can resist node replication attacks in a localized fashion. Note that, compared to the distributed algorithm, which only requires that nodes perform the task without the intervention of the base station, the localized algorithm is a particular type of distributed algorithm. Each node in the localized algorithm can communicate with only its one-hop neighbors. This characteristic is helpful in reducing the communicationoverhead significantly and enhancing the resilience againstnode compromise.

•Efficiency and Effectiveness: The XED and EDD algorithms can identify replicas with high detection accuracy. Notably, the storage, communication, and computation overheads of EDD are all only O(1).

• Network-Wide Revocation Avoidance: The revocation of the replicas can be performed by each node without flooding the entire network with the revocation messages.

• Time Synchronization Avoidance: The time of nodes in the network does not need to be synchronized.

5.2 XED

In eXtremely Efficient Detection (XED), the basic operations of this protocol are as follows: Once two sensor nodes encounter each other, they respectively generate a random number, and then exchange the random numbers. If the two nodes meet again, both of them request the other for the random number exchanged at earlier time. If the other cannot reply or replies a number which does not match the number stored in its memory, it announces the detection of a replica.

To a smart attacker, this scheme is weak, and he/she can establish secret channels among replicas. By this way, replicas can share the random numbers, and make the protocol fail.

Only constant communication cost O (1) is required and the location information of sensor nodes is unnecessary.The effectiveness of XED, unfortunately, heavily relies onthe 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 neighboring replicas, thus degrading the detection capability because multiple replicas are able to reply with the correct random number to encountered genuine nodes accordingly. This weakness will be solved in EDD.

5.3 EDD

The basic idea behind Efficient and Distributed Detection (EDD) scheme is:
1) For 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.
2) For a network with two replicas v, the number of times μ_2, that u encounters the replicas with a same ID 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 composed of two steps: off-line and on-line. Off-line step is performed by the network planner before sensor deployment, to calculate the parameters time period T and threshold. Online step performed by each node per move. Each checks whether the encountered nodes are replicas by comparing threshold with number of encounter at the end of time interval T. This schemes leads to storage overhead since, each node should maintain list L.

TABLE 1: Memory Consumption of the Proposed Schemes

	ROM	RAM
XED	13434 Bytes	633 Bytes
EDD	11418 Bytes	531 Bytes

TABLE 2: Detection Speed of the Proposed Schemes

	Detection Speed
XED	0.25 seconds
EDD	0.043 seconds

6 Performance Evaluation

Five performance metrics are used in our evaluation:

i) Detection Accuracy—Detection accuracy is used to represent the false positive ratio and false negative ratio of the underlying detection algorithm, which are the ratios of falsely considering a genuine node as a replica and falsely considering a replica a genuine node, respectively.
ii) Detection Time—Detection time is evaluated according to the average time (or, equivalently, the number of moves) required for a genuine sensor node u to add the replica's ID into $\beta^{(u)}$.
iii) Storage Overhead—Storage overhead is counted in terms of the number of records required to be stored in each node. Here, the records differ in different algorithms. For example, a record is a tuple containing an ID, time, location, and signature in while a record involves only an ID, location, and signature in If the storage overhead is counted in terms of the number of bits, a multiplicative factor O(log n) is obviously needed due to the space for IDs. Nonetheless, for fair comparison, we do not use such bit-based storage estimation.
iv) Computation Overhead—Computation overhead accounts for the number of operations required for each node to be executed per move.
v) Communication Overhead—Communication overhead accounts for the number of records required for each node to be transmitted. Similarly, it can be considered in terms of the number of bits, but we do not use such a kind of estimation.

TABLE 3: Detection Mechanisms Performance Overheads

Schemes	Communication Cost	Memory
SET	O (n)	O (d)
Node-to-Network (Broadcast)	O (n^2)	O (d)
Randomized Multicast	O (n^2)	O ($\sqrt{n}$)
Line-Selected Multicast	O ($n\sqrt{n}$)	O ($\sqrt{n}$)
SDC	O ($r_f \sqrt{n}$) + O(s)	g
P-MPC	O ($r_f \sqrt{n}$) + O(s)	g
XED	O (1)	--
EDD	O (1)	1

Where,

n- Number of nodes in Network

d- Degree of neighbouring nodes

g- Number of witness nodes

r- Communication radius

r_f- Number of neighbouring nodes forwards location claims.

As future work, we can enhance localized algorithms with facilitate on Zone Routing Protocol which splits Mobile WSN as more number of Zones. In each zone, leader node will be generated by this protocol as dynamically at regular time periods for detect replicas as efficiently.

7 Conclusion

Based on the assumption that a sensor node, when attempting to join the network, must broadcast a signed location claim to its neighbors, most of the existing distributed detection protocols adopt the witness-finding strategy to detect the replicas. In particular, the general procedure of applying witness-finding to detect the replicas can be stated as follows. After collecting the signed location claims for each neighbor of the node , where and denote the location of and the digital signature function respectively, sends the collected signed location claims to a properly selected subset of nodes, which are witnesses. 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, network-wide revocation.

ACKNOWLEDGMENT

We are sincerely thankful to the Head of the Department and all Teaching Staff Members of Information Technology and Electronics and Communication Engineering for support and guidance and we also like to thank the management of P.B. College of Engineering for their support for carry out this work efficiently.

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 Trans. Syst., Man, Cybern. C, Applicat. Rev., 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] G. Cormode and S. Muthukrishnan, "An improved data stream summary the count-min sketch and its applications," J. Algorithms, vol.55, no. 1, pp. 56–75, 2005.

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

[5] 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.

[6] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in Proc. Int. ICST Conf. Security and Privacy in Communication Networks (Securecomm), Nice, France, 2007, pp.341–350.

[7] 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.

[8] J. Ho, M. Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), Brazil, 2009, pp. 1773–1781.

[9] R.A.Johnson and D.W.Wichern, Applied Multivariate Statistical Analysis. Englewood Cliffs, NJ, USA: Prentice-Hall, 2007.

[10] T. Karagiannis, J. L. Boudec, and M. Vojnovic, "Power law and exponential decay of inter contact times between mobile devices," in Proc. ACM Int. Conf. Mobile Computing and Networking (MobiCom), Montreal, Canada, 2007, pp. 183–194.

[11] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: A secure sensor network communication architecture," in Proc. Int. Conf. Information Processing in Sensor Networks (IPSN), Cambridge, MA, USA,2007.

[12] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in Proc. Int. Conf. Information Processing in Sensor Networks (IPSN), Berkeley, CA, USA, 2004, pp.259–268.

[13] C.-M. Yu, C.-S. Lu and S.Y. Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in Proc. IEEE Vehicular Technology Conf. Fall (VTC-Fall), Anchorage, AK, USA, 2009, pp. 1–5.

[14] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks," inProc. IEEE Symp. Security and Privacy (S&P), Oakland, CA, USA, 2004, pp. 259–271.

[15] 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.