International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 2 (2014), pp. 153-164

http://www. irphouse.com /ijict.htm

Towards Techniques of Detecting Node Replication Attack in Static Wireless Sensor Networks

Moirangthem Marjit Singh[1], Ankita Singh[2] and Jyotsna Kumar Mandal[3]

[1,2] Department of Computer Science & Engineering, North Eastern Regional Institute of Science & Technology, Arunachal Pradesh, India.
[3]Department of Computer Science & Engineering, University of Kalyani, West Bengal, India.

Abstract

The paper reports the techniques to detect node replication also called clone node attacks in the Static Wireless Sensor Networks (sWSN) and critically reviews them. The focus of the paper is to highlight and discuss various techniques to deal with node replication attack in static WSNs.

Keywords: WSN; security; node replication attack.

1. Introduction

Wireless Sensor Networks (WSNs) are specialized network of large number of sensor equipped nodes which are spatially deployed over the region of interest where the nodes may be stationary or mobile in nature. Wireless sensor networks are a group of small untethered sensor devices which are densely populated in a specific target area, where they collaborate in an ad-hoc manner to sense phenomena and report sensed data for various uses [8]. Sensor nodes are vulnerable to a number of attacks and hence its security can be compromised by an attacker. The node replication attack or the clone node attack is a security threat where an attacker creates its sensor nodes and joins the network as if they are the legitimate nodes of the network. For this attack to happen, the attacker will physically capture one node from the network and extract all the secret information of the node such as node ID, Keys etc.Using the extracted information, the attacker creates many replicas/clones of the compromised node. These clones are then deployed into the WSN at suitable positions and start to attack the whole network internally [1] which will hamper the network. The nodes are stationary or fixed for the static WSNs and hence the node's location/position does not change

after deployment. This is in contrast to the mobile WSNs where the nodes are mobile in nature and hence the position of the node changes. The node operates while controlling their own movement [1]. As a result, the techniques to detect node replication attack are different for static and mobile WSNs. A number of protocols for detecting node replication attack in static WSNs can be found in the literature**.** Some of which are discussed in this paper. Section 2 of the paper deals with the detection techniques and conclusions are drawn in section 3.

2. Node Replication Detection Techniques for Static Wireless Sensor Network

2.1. Node to Network Broadcasting

This protocol is developed by Parno et al[2]. In this protocol each node floods the entire network with its location claim. It is assumed that each node is aware of its location. Each node in the network stores the location claim of neighboring node and in case of conflicting claims, revokes it.

2.2. Deterministic Multicast

Developed by Parno et al[2], this protocol is an enhancement to the node to network broadcast protocol[2]. Here limited number of witness nodes, chosen deterministically, stores the location claims. When a node broadcasts its location claims, the neighboring nodes forward these claims to the witness nodes. The witnesses are chosen as functions of node's ID [2] hence the replicated node having the same ID will reach the same witness node and the witness node will receive conflicting location claims and hence the revocation process can be initiated.

2.3. Randomized Multicast

This protocol was developed by Parno et al to increase the resiliency of deterministic multicast [2]. Unlike the deterministic multicast where the selection of witness node was done in a deterministic manner depending upon the IDs of the nodes, in Randomized multicast, the node location information are distributed randomly to selected witness nodes in such a manner that the attacker cannot predict their identities[2]. At a high level, the protocol has each node broadcast its location claim along with a signature authenticating the claim [2]. Each of the node's neighbors probabilistically forwards the claim to the set of witnesses if any witness receives a conflict the node can be revocated. The birthday paradox ensures that the clone node gets detected with high probability using a relatively limited number of witnesses [2].

2.4. Line Selected Multicast

To further reduce the communication cost of randomized multicast, Parno et al proposed another protocol called line select multicast [2].. This protocol takes into account the property that each node behaves both as a sensing node and a router while forwarding the location claims. Here the intermediate node through which the location

claims passes should also store the claims [2] and while forwarding some other claim if it encounters a conflict a revocation process can be initiated.

2.5. Fast and Scalable Key Establishment in Sensor Networks

T Dimitriou et al [3] have proposed a fast and scalable key establishment protocol which is resilient to node replication. Here sensor nodes are assigned a unique ID that identifies them in the network, as well as three symmetric keys[3], where first key, is shared between each node and the base station, this key is used to secure information sent from a node to the base station. Second key, shared between each node and the base station, this key is used only by those nodes that will become cluster heads and it becomes the cluster key. The third key is the master key shared among all nodes, including the base station, this key is used to secure information exchanged during the cluster key setup phase and is erased from the memory of the sensor nodes[3]. The cluster key setup procedure is divided into two phases: organization into clusters and secure link establishment [3]. During the first phase the sensor nodes are organized into clusters and agree on a common cluster key, while in the second phase, secure links are established between clusters in order to form a connected graph [3]. An implicit assumption here is that the time required for the underlying communication graph to become connected (through the establishment of secure links) is smaller than the time needed by an adversary to compromise a sensor node during deployment [3]. Here all the communication is done by encrypting the message using the master which is erased soon after the establishment of secure link. This provides Resiliency against node capture and replication [3].

2.6. Localized Encryption and Authentication Protocol (LEAP)

Sencun Zhu *et al* [4] have proposed an efficient security mechanism for large scale distributed sensor network called LEAP. LEAP is capable of defending against node replication attack. It handles the establishment of four types of keys [4] for each node i.e. an individual key, a pair-wise key, a cluster key and a group key. The individual key is shared with the base station and the pair-wise key is shared with another node. The cluster key is shared with all the neighboring nodes and the group key is shared with all the nodes of the network. The controller or the base station generates an initial key which is unique and loads each node with the unique initial key[4] and each node then derives a master key using the pseudo random function[4] preloaded in it. The protocol is based on a reasonable assumption that $T_{min} > T_{est}$ [4], where T_{min} is the time taken by the adversary to compromise a node and T_{est} is the time taken by a node to discover its neighbor. Soon after deployment the node sets a timer and starts the process of neighbor discovery and establishing secure link with the neighbors. During the neighbor discovery phase each node computes the master key of its neighbor using its initial key which is used to establish the pair-wise key and as the secure link is established the initial key and the neighbor's master keys are erased hence any compromised node which tries to establish a secure link after T_{est} fails to do so and the network is secure against node replication attack.

2.7. C. Bekara and M. Laurent-Maknavicius have proposed a new protocol in[5].
In this protocol, the pair-wise key establishment is done by using symmetric polynomial and the nodes are deployed in groups belonging to different generations where each group or generation is deployed at fixed time interval. This protocol also assumes that the time taken by the adversary to compromise a node T_{comp} [5] is greater than the time taken by the nodes to establish a secure link with other nodes $T_{est.}$[5]. Initially the base station generates a random symmetric bivariate polynomial and loads the node with its share of polynomial obtained by passing the first argument of the polynomial as defined in the protocol. Each node has a unique share. The process for neighbor discovery starts when a node of either the same generation or of younger generation requests for link establishment. So a clone node of older generation fails to join the network with an exception of the case when it responds to a newly deployed node.

2.8. Randomized Efficient and Distributed (RED) Protocol
M. Conti *et al* in [6] have proposed the RED protocol which is randomized, efficient and distributed. Extensive simulations of RED show that it is highly efficient with regards to required communications, memory, and computations and moreover, as compared to other distributed protocols, it sets out improved attack detection probability [6]. RED executes at fixed intervals of time. This protocol runs in two steps [6]. In the first step, a random value is shared among all the nodes. This can be performed with centralized broadcasting, or with distributed mechanisms. During second step, each sensor node will digitally sign and broadcasts its claim that includes node ID and geographic location [6]. For each node, each of its certain neighbors forwards the claim to more than 1network locations as mentioned in [6].The set of witness nodes is selected using the *PseudoRand* function[6]. The claim message is signed by each node with its private key before sending it. For each received claim, the potential witness node verifies the received signature then checks for the freshness of message. If the check is passed the witness node extracts the information (*ID* and location)[6] and it checks whether this is the first received claim carrying *ID*, if so then it simply stores the messages otherwise the witness checks whether the claimed location is the same of the stored claim for this *ID*. If it is not, the witness node triggers a revocation procedure for the given ID.

2.9. Hierarchical Node Replication Detection in Wireless Sensor Networks
Znaidi et al have proposed an algorithm for detecting node replication attacks using a Bloom filter mechanism. This algorithm depends on a cluster head selection that is performed using LNCA (local negotiated clustering algorithm) protocol [7]. The detection of node replication attack is done with the exchange of node IDs through a bloom filter with the other cluster heads. This algorithm works in three steps. Prior distributions of all the materials required for Bloom filter computations and for the cryptographic operations are done in the first step. It selects the cluster head in the

second step. Bloom filter construction and verification are done in the third step by each cluster head and other cluster heads respectively [7].

2.10. Ho et al have proposed a distributed detection method in[8]

The key assumption in the work is the use of a group deployment strategy. In this strategy, sensor nodes are deployed in groups, with each group of nodes being deployed towards the same location, called the *group deployment point* [8]. The deployment follows a certain probability density function (pdf) f [8], which describes the likelihood of a node being a certain distance from its group deployment point. For simplicity, they use a two-dimensional Gaussian distribution to model f [8]. The authors have proposed three schemes of detection. The schemes are the basic approach [8], the location claim approach [8] and the tree based approach [8] and an addition protocol called deployment time check [8] can be used to increase the efficiency of the schemes.

Scheme I: The basic scheme, assumes that sensor nodes are deployed group by group, and that each group is expected to be deployed towards a deployment point that can be pre-determined [8]. Prior to deployment, the network operator loads the pre-determined deployment coordinates of every group onto every sensor node. It is noted that the sensor nodes in the same group are very likely to be close to each other after deployment. The sensor nodes in the network are divided into groups, and each group has a unique group ID. The ID of every sensor node has two parts: the group ID and a unique ID within the group [8]. Keying materials are also pre-loaded to each sensor node for pair-wise key establishment, any key pre-distribution technique can be used for sensor networks [8]. When a sensor node receives a request from its neighbor node to forward a message after deployment it checks whether or not the distance between the deployment points of groups to which the two nodes belong is smaller than a pre-defined system wide threshold [8]. If the condition is fulfilled, the neighbor node is believed to be a trusted node and it's message is forwarded. Otherwise, every message from that neighbor node is ignored.

Scheme II: In Location claim approach, in addition to the keying materials for pair-wise key establishment, every sensor node also gets the keying materials for generating digital signatures [8]. The deployment zone of a group is defined as a circle centered at the group's deployment point with a certain radius [8]. After deployment, every node discovers its real location and produces a location claim. In neighbor discovery phase every sensor node discovers a set of neighbor nodes. If a neighbor node claims a location such that the distance between the location of the node and it's neighbor is larger than the assumed signal range then that neighbor will be removed from the neighbor list and the node then

checks for every neighbor node whether or not it is deployed in the right place [8]. If the check fails for a certain neighbor node it will be marked un-trusted[8]. A sensor node always forwards message received from its neighbors whether trusted or un-trusted. However in case of un-trusted neighbor its location claim is sent to its home zone[8] for replica detection. The location claim after reaching the home zone is flooded throughout the home zone and any node receiving a conflicting claim can conclude that the node has been replicated.

Scheme III: This is a tree based scheme where every sensor node forwards every location claim to a number of groups instead of a single group [8]. The proposed approach in the following is similar to Scheme II. The only difference is in the way the group is selected to which the location claims are sent. For a certain group say 'x', the protocol organizes the set of groups into a complete virtual binary tree[8] with the group 'x' as its root and the position of other groups in the tree is determined in a pseudo-random way based on a seed[8]. In case a node encounters an un-trusted neighbor, its location claim is sent upwards the tree to all the groups till it reaches the root.

2.11. Yingpei Zeng et al have proposed two non deterministic fully distributed and random walk based approaches in[9].

The protocols/ approaches as described in [9] are RAWL (RAndom WaLk**)** and TRAWL (Table-assisted Random WaLk**)**. The protocols assume the nodes to be uniformly distributed in the deployment field and that each node knows their own locations.

RAWL:Each node *a* broadcasts a signed location claim to its neighbors. When hearing the claim, each neighbor verifies the signature and checks the plausibility of the location claim. Then with probability *p*, each neighbor randomly selects *g* nodes (or *g* locations) and uses geographic routing to forward the claim to the *g* nodes [9]. Each chosen node that receives the claim of *a*, first verifies the signature. Then it stores the claim and becomes a witness node of *a*. The neighbor will also become a witness node of *a*. It adds counter by one and continues to forward the message to a random neighbor, unless counter reaches *t* [9]. When a node finds a collision (two different location claims with a same node ID), the node will broadcast the two conflicting claims as evidence to revoke the replicas. Each node receiving the two claims independently verifies the signatures. If the two signatures are valid, it terminates the links with replicas [9].

TRAWL: This protocol is modified from RAWL [9]. When a randomly chosen node performs a random walk, all the nodes that are passed through will become witness nodes. However, they will store the location claim independently with certain probability [9]. Also, each witness node creates a new entry in its table so as to record the pass of a location claim. Every entry of the table maintained by each node corresponds to the pass of a random walk (with a location claim). The table has the two

columns: NodeID[9] and ClaimDigest[9]. The claimDigest can be computed by using a random value generated by each node itself to prevent the adversary from generating a false claim with the same digest value [9]. On receiving a location claim, a node first finds the entries which have the same node ID as the claim in its trace table. Then if any entry is found, the node will compute the digest of the claim as explained in [9] and compares the digest with the digest in the entry. When the two digests are different, the node detects a clone attack [9].

2.12. Localized Multicast

B. Zhu et al [10] have proposed a novel distributed protocol for detecting node replication attacks called localized multicast that takes a different approach for selecting the witness nodes [10]. The random selection of witness nodes for the node identity from the nodes that are located within a limited region called a cell [10] is performed. First the node ID's are deterministically mapped to one or more cells and then randomization is done within the cells to increase the resiliency and security of the scheme. There are two variants of this protocol [10] namely SDC (Single Deterministic Cell) and P-MPC (Parallel- Multiple Probabilistic Cells**)**. Every sensor node is allotted a unique identification number and a pair of identity-based public and private keys. This is done by an offline Trust Authority (TA) [10]. To generate a new key pair, cooperation from the TA is must hence here it is assumed that adversaries cannot easily create sensors with new identities and hence fails authenticate itself [10]. In SDC, the unique and random mapping of node id to one of the cells in the grid is performed using a geographic hash function. Whenever a node transmits its location claim, every neighboring node first verifies the plausibility of the location and the validity of the signature in the location claim [10]. When the neighbor node forwards the claims, it executes the geographic hash function to determine the destination cell 'D'. Once the location claim arrives at the cell, the node receiving the claim verifies the validity of the signature firstly and then checks whether cell D is indeed the cell corresponding to that identity included in the claim message, when verified the entire cell is flooded with the claim. Whenever a witness receives a conflicting claim it informs the base station which initiates the revocation process. Like SDC, in P-MPC [10] a geographic hash function is used to map sensor node's location claim to the destination cell, however instead of mapping to single cell, in this protocol the location claim is mapped to multiple cells. The detection and revocation process is carried on the basis of the result of the witness nodes same as in SDC [10].

2.13. A Range-based Detection Method (RBDM) of Replication Attacks in Wireless Sensor Networks

Range based detection method is proposed by Huang Jian et al [11]. They proposed to design a new distributed approach which does not require any nodes geographic position messages or system time synchronization for detecting the node replication or the clone attacks in wireless sensor networks [11]. The fundamental idea is to make use of the unique identification property: If a node has been detected, it could not

appear in any other area. The RBDM is a range-based distributed detection method. In this paper, they used RSSI (received signal strength indicator) to estimate the distance between nodes. Each node estimates the distances between it and its neighbors by RSSI and executes a test for categorizing the neighbors as follows [11]: assuming two nodes *a* and *b* and the detection range R. These nodes are categorized as close neighbors if distance between nodes $|x_a - x_b| \leq R$ as mentioned in [11]. RSSI is used as a distance estimator for Range-based detection. If the distance between the nodes $|x_a - x_b| \leq R/2$ then they are categorized as far neighbors[11]. Each node records all identifications of its neighbors and set a flag signify their categorization. All of this information is stored in the neighbor-information table. Nodes in the network periodically broadcast own neighbor information table. By comparing node's neighbor-information table, the replication attacks can be detected. Three criterion are suggested in the proposed protocol namely Local Unique ID Criterion [11], which is used to detect clone node in the neighborhood of the compromised node itself. Neighbor Unique ID Criterion [11], which is used if the clone node and the compromised node are in the neighborhood of another node. Global Unique ID Criterion [11], which is used when the clone node and the compromised nodes are placed sparsely.

2.14. Ho, Jun-Won have proposed a sequential hypothesis in [12] for detection of replica cluster

Replica cluster is a special case of replication where multiple replicas with the same identity and secret keying materials are placed in the same small regions forming a cluster [12]. In the proposed work each node performs the SPRT (Sequential Probability Ratio Test) on its neighbor node. This is done using the null hypothesis that a replica cluster of the neighbor node does not exist. The alternate hypothesis is that a replica cluster of the neighbor node exists [12]. In SPRT, if the number of communication peers of a neighbor node is less or exceeds a pre-configured threshold value, it will lead to the acceptance of the null or alternate hypotheses respectively. As soon as the alternate hypothesis is accepted, the node will stop communicating the neighbor node [12].

2.15. ComSen: A Detection System for Identifying Compromised Nodes in Wireless Sensor Networks

As proposed by Yi-Tao Wang and Rajive Bagrodia in [13] this protocol detects the replication depending on the behavior of the neighboring nodes. It focuses on monitoring communications for misbehavior. Misbehavior is decided using anomaly-based or rule-based approaches [13]. Anomaly-based approaches establish a baseline behavior for neighbors and consider behavior that deviate from the baseline as anomalous. Rule-based approaches detect misbehavior as soon as a condition, established before deployment of the network, is met. ComSen uses a hybrid approach [13], consisting of two components: a distributed system running on every node in a WSN and a centralized system running on the base station. ComSen only monitors

some common features in WSNs such as sensor reading, receive power, send rate, receive rate [13].

The comparison of various techniques for the detection of node replication attack that are reviewed in the paper is given in table 1 and the notations used are described in table 2.

Table 1: Comparison of various detection techniques.

Technique	Location aware	Category	Computation cost	Memory cost	Detection rate
Node to network broadcasting	Yes	Distributed	O(n2)	O(d)	100%
Deterministic multicast	Yes	Distributed	O(g log(n)1/2 /d)	O(g)	--
Randomized multicast	Yes	Distributed	O(n2)	O(n)1/2	95%
Line select multicast	Yes	Distributed	O(n(n)1/2)	O(n)1/2	95%
Fast and scalable key establishment in WSN	No	Distributed	--	--	--
LEAP	No	Distributed	--	--	--
A new protocol by C.bekara and M. Laurent-Maknavicius	No	Distributed	O(n)1/2	O(d)	--
RED	Yes	Distributed	O(r(n)1/2)	O(r)	90%
Hierarchical Node Replication Detection	No	Hierarchical	O(t2)	O(t)	--
Ho et al proposed distributed detection method	Yes	Distributed	--	--	---
Random walk based RAWL Approaches TRAWL	Yes Yes	Distributed distributed	O((n)1/2 log(n)) O((n)1/2 log(n))	O((n)1/2 log(n)) O(1)	-- --
Localized multicast	Yes	Distributed	--	--	--
Range based detection method	No	Distributed	--	--	--
Sequential hypothesis for replica detection	No	Distributed	O(n)	O(d)	--
ComSen	No	Hybrid	--	--	99%

Table 2: Notations.

n	number of nodes in the WSN
d	degree of neighboring nodes
g	number of witness nodes
t	number of cluster heads
r	communication range/radius
--	Not available

3. Conclusion

The paper has presented a brief review on various node replication attack detection techniques/protocols for static WSNs. The techniques reviewed in the paper fall in two categories namely location aware and location independent protocol. Location aware protocols require the nodes to know their geographic location for which the nodes should either have GPS or must rely on the base station to compute their location coordinates. The location independent protocol does not require the knowledge of the nodes' location to detect node replication. The performance of these protocols/techniques depends on the density of the networks as reported in the literature. Hence research in this area is required to address this issue.

References

[1] WZ Khan, Mohammed Y. Aalsalem, Mohammed Naufal Bin Mohammed Saad, and Yang Xiang, "Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey", International Journal of Distributed Sensor Networks ,Volume 2013, Article ID 149023, 22 pages,2013

[2] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proceedings of the IEEE Symposiumon Security and Privacy *(IEEE S and P '05)*, pp. 49–63, May 2005.

[3] Tassos Dimitriou, Ioannis Krontiris and Fotios Nikakis, "Fast and scalable key establishment in sensor networks." Shashi Phoha, Thomas F. La Porta, and Christopher Griffin, editors, Sensor Network Operations: Wiley-IEEE press, pp 557-570, 2006

[4] Sencun Zhu, Sanjeev Setia, Sushil Jajodia. LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In The Proceedings of the 10th ACM conference on Computer and communications security *2003.*

[5] C. Bekara and M. Laurent-Maknavicius, "A new protocol for securing wireless sensor networks against nodes replication attacks," in Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '07),White Plains, NY, USA, October 2007

[6] 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 Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc ’07), pp. 80–89, September 2007.

[7] Znaidi, Wassim, Marine Minier, and Stéphane Ubéda. "Hierarchical node replication attacks detection in wireless sensors networks." In Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on, pp. 82-86. IEEE, 2009.

[8] Ho, Jun-Won, Donggang Liu, Matthew Wright, and Sajal K. Das. "Distributed detection of replicas with deployment knowledge in wireless sensor networks." In Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on, pp. 1-6. IEEE, 2009.

[9] Yingpei Zeng, Jiannong Cao, *Senior Member, IEEE,* Shigeng Zhang, Shanqing Guo and Li Xie,“Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks”, IEEE Journal On Selected Areas In Communications, Vol. 28, No. 5, June 2010

[10] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L.Wang, “Localized multicast: efficient and distributed replica detection in large-scale sensor networks,” IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 913–926, 2010

[11] Huang Jian, Xiong Yan, Li Ming-xi, Miao Fu you, “A Range-based Detection Method of Replication Attacks in Wireless Sensor Networks”, International Conference on Information and Computer Networks 2012, vol. 27

[12] Ho, Jun-Won. "Sequential Hypothesis Testing Based Approach for Replica Cluster Detection in Wireless Sensor Networks." Journal of Sensor and Actuator Networks 1, no. 2 : pp153-165, 2012.

[13] Yi-Tao Wang and Rajive Bagrodia,” ComSen: A Detection System for Identifying Compromised Nodes in Wireless Sensor Networks”, SECURWARE 2012 *:* The Sixth International Conference on Emerging Security Information, Systems and Technologies,2012