Indian Journal of Science and Technology, Vol 8(16), DOI: 10.17485/ijst/2015/v8i16/54150, July 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Detecting Node Replication Attacks in Wireless Sensor Networks: Survey

L. Sujihelen[1*], C. Jayakumar[2], C. Senthil Singh[3]

[1]Assistant Professor, Faculty Of Computing, Sathyabama University, Chennai, India,sujihelen@gmail.com
[2]Professor, Department Of C.S.E, R.M.K. Engineering College, Chennai, India,cjayakumar2007@gmail.com
[3]Associate Professor,Toch Institute of Technology, Ernakulam,India, senthilsingh@gmail.com

Abstract

Wireless Sensor Networks has collection of sensor nodes. The sensor nodes may be captured by the attacker because the nodes are spread out in unattended surroundings. The attacker collects all secret information such as key, secret credentials, etc. and replicates the node. This replicated node is also called as Clone node. In this paper, an attack called as node replication attack is discussed. The clone node or replicated node behaves as a legitimate node. The clone node can damage the network. In node replication attack, detecting the clone node is an important issue in Wireless Sensor Networks. In this survey, the existing detection schemes by researchers are discussed.

Keywords: Centralized, Distributed, Mobile WSN, Node Replication Attacks, Security, Static WSN

1. Introduction

Wireless Sensor Networks has collection of Sensor Nodes. It is used in more applications such as environmental monitoring, habitat monitoring and object tracking. The sensor nodes may be captured by an adversary because the sensor nodes are spread out in unattended surroundings. The main common attacks in sensor network are clone attack, man in the middle attack, Sinkhole, Jamming, tampering, flooding, wormhole attack, routing attack, sybil attack, Denial of Service attack. The different types of attacks are shown in Figure 1.

In this paper, a severe attack in WSN called as Node Replication Attack is dicussed. In this attack the adversary access the internal state of the sensor node such as Secret information, key, etc. After getting the key the adversary can easily replicate the node. The duplicated node can be inserted into any location in the network. If the replicated node is not detected, then it leads to different attacks. The clones extract information from the network and collects all the secret information. And also it disconnects the network or jamming the network, which leads to Denial of Service attack. Some times the replica node leads to worm whole attack, the attacker tunnels the packet received and send in another way in the network and replays the packet. The replication attacks injurious in many parts of the networks such as misbehavior activities, extra resource allocation, falsifying sensor data etc.

Figure 2 shows the replicated node in the sensor networks. Detecting Replicated node is a difficult task. For detecting the node replication attacks a few schemes have been proposed. The proposed detection technique should be energetic and memory demanding because the sensor nodes are resource constrained.

In this paper the node replication attacks is organized in the second section. The various detection schemes for static and mobile WSN are discussed in section 3, 4 and the conclusion, references are discussed in 5 and 6.

2. Node Replication Attacks

In the node replication attacks the adversary captures the sensor node and extract the secret credentials. After extracting the secrets, duplicate the node and deploys in the duplicated node in the network. The duplicate node is called as clone nodes or replicated nodes. The clone

*Author for correspondence

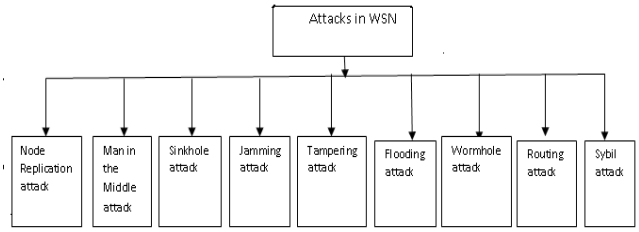

Figure 1. Different types of attacks in wireless sensor network.

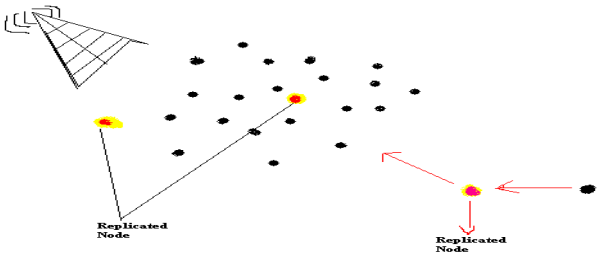

Figure 2. Node replication attack.

nodes or replicated nodes behave as an original node. The Wireless Sensor Networks can be static or mobile. In static WSN, the mobile nodes are deployed randomly. After deployment the mobile node locations cannot change. But in Mobile WSN the sensor nodes are deployed randomly but its have mobility or it moves on their own place. In Static WSN, a sensor node has a unique location id. By using centralized schemes easily the replicated node is detected. In Mobile WSN its location id is varying due to roaming. The different detection technique is proposed for Mobile WSN.

3. Detection Schemes for Static WSN

Many schemes are proposed for detecting this attack. In static wireless sensor networks, the different types of detection schemes are categorized based on Centralized, Distributed Approach. The different detection schemes are shown in the Figure 3.

3.1 Static WSN for Centralized Approaches

Detecting clone nodes in static WSN for centralized Approach is a simple task. In a centralized approach mainly the base station is responsible for monitoring all the nodes. If any replicated node is present then

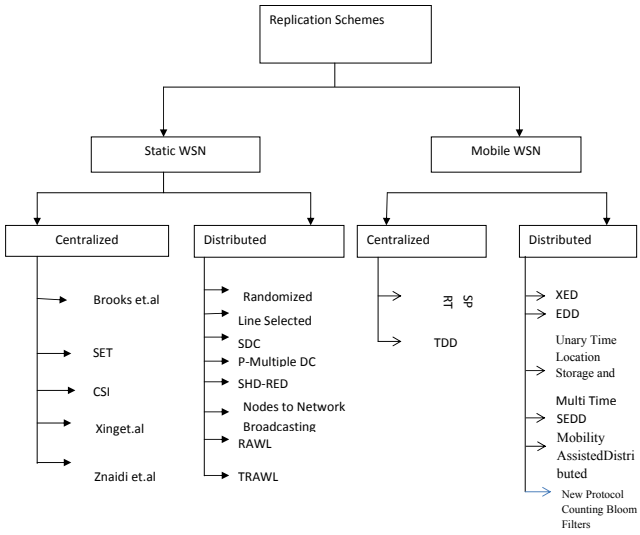

Figure 3. Detection schemes in node replication attack.

monitoring node sends an alarm message. For centralized approach, some of the detection schemes have been analyzed. The detection schemes are discussed below and the communication cost and memory for each detection scheme is shown in the Table 1.

3.1.1 *Using Random Key Predistribution*

Brooks et al.[1] proposed the node replication detection technique on Random Key Predistribution. Here the key predistribution scheme is used. This predistribution scheme follows some conditions. If the usage of keys exceeds the criteria or threshold value, then it is assigned as a replicated node. The bloom Filter technique is used.

Table 1. Detection Scheme in Static WSN for Centralized Approaches

Detection Schemes	Communication cost	Storage cost
Brooks et al.[1]	O(n log n)	
SET	O(n)	O(d)
CSI	O(n log n)	
Xing et al.[15]	C(1+ ratio)	O(d)+min(M,w)
Znaidi et al.[5]	$O(t^2)$	O(t)

n-no.of nodes in the network, w-column weight in s-disjunct code, C-message generated by node, d-degree of neighbouring nodes, M-number of rows, s-disjunct code.

The BS (Base Station) counts the total number of times the key is accessed.

3.1.2 SET

Choi et al.[1,2] proposed a scheme SET to identify the clone nodes. In this scheme the network is divided into different subsets. Each subset has separate leader. The Subset Leader (SL) sends the information to the base station. The intersection operation is used on root node of the sub tree for finding clone nodes. If the intersection set is empty, then there are no clone nodes.

3.1.3 CSI (Compressed Sensing based Clone Identification in Sensor Networks)

Lu et al.[3] proposed the scheme called CSI. In this scheme, each node senses some information and forwards to the neighbor node. The base station receives the sensed data from the node. Here one threshold value is fixed (α). If the sensor node has the sensor reading greater than the fixed value then that node is assigned as a clone node.

3.1.4 Realtime Detection of Clone Attacks in Wireless Sensor Networks

Xing et al.[4] proposed a detecting clone node in sensor networks. Each sensor computes the fingerprint with the nearest node characteristics. Each node verifies by checking the fingerprint. The verification is with base station and the nearest sensors, which has high detection rate.

3.1.5 Znaidi et al. - Hierarchical Distributed Algorithm

Zinaidi[5] proposed a scheme using a Bloom technique. Three phases are there in this scheme, predistribution phase, Election phase, Detection phase. In the predistribution phase, node id is assigned to all the nodes. In the Election phase, Cluster head is elected. Each cluster head use the bloom filter for detecting the clone nodes. The verification is performed by other cluster head.

3.2 Static WSN for Distributed Approaches

In distributed techniques, there is no central authority to monitor. But the information is sent to the node which is selected randomly called as witness node. The different types of detection schemes are shown in the Table 2.

Table 2. Detection Scheme in Static WSN for Distributed Approaches

Detection Schemes	Communication Overhead	Storage Overhead
Randomized Multicast (parno et al.[6])	O(n)	O(P√n)
Line-Selected Multicast Protocol	O(n√n)	O(√n)
SDC(single Deterministic Cell Scheme	$O(r_c . \sqrt{n})+O(s)$	w
P-multiple DC	O(r. √n)+O(s)	w
SHD(Single Hop Detection)-RED	O(g.p.d.n√n)	O(g.p.d)
Nodes to Network Broadcasting	$O(n^2)$	O(1)
RAWL	$O(\sqrt{n} \log n)$	$O(\sqrt{n} \log n)$
TRAWL	$O(\sqrt{n} \log n)$	O(1) 2

n – No. of nodes, d – Degree of neighbouring nodes, g - No. of witness nodes, rc – No of neighbouring nodes forwards location claims, s - The number of sensors in a network.

3.2.1 Randomized Multicast (Parno et al.)

Parno et al.[6] proposed RM technique, when a node broadcasts its location all the neighbour nodes send a signed copy of location claim. If a node detects the other node with different locations at the same time, then it is called as witness. It has a high communication cost, but the security is increased.

3.2.2 LSM (Line Selected Multicast Protocol)

Parno et al.[6] proposed to reduce the communication cost of RM, so the LSM is introduced. In LSM the communication cost is reduced, but the energy is depleted.

3.2.3 SDC (Single Deterministic Cell Scheme)

Zhu et al.[7] proposed SDC scheme the node is mapped to the location of each node. The cell stores the node's witnesses with some probability.

3.2.4 P-multiple DC

Zhu et al.[7] proposed a P-Multiple DC, each node with the ID is map to multiple cells. In P-MPC a hash function is used to map from node identity to the destination cells.

3.2.5 SHD (Single Hop Detection)-RED

Conti et al.[8] proposed a detection protocol which is to solve the problem as the selection of witness nodes is random and

fully distributed. The witness nodes are selected in pseudo random who lead to a uniform witness distribution. The main drawback of RED is the selection of witness nodes. This scheme is not able to detect masked replication attack.

3.2.6 Nodes to Network Broadcasting

Parno et al.[6] scheme explains about broadcasting the location of the node to the whole network. All nodes store the neighbour nodes locations. The clone node is identify based on node ID.

3.2.7 Random Walk (RAWL)

Zeng et al.[9] proposed a Random Walk (RAWL) scheme randomly walk in the network and selects the past nodes as the witness nodes. In this method the node broadcasts a signed location claim. The node neighbour sends the claim to some selected nodes is followed in next step. Next the nodes are selected randomly for starting the random walk. Then assign the passed nodes as a witness nodes and will store the claim. The same node has different location, then it revokes the replicated node is done in last step.

3.2.8 TR AWL (Table-Assisted Random Walk Based Detection)

Zeng et al.[9] proposed a TRAWL. TRAWL stores all the information such as location claims, the size of a table. But the size of the table entry is smaller than the size of a location claim. The passed nodes are assigned as witness nodes.

4. Detection Schemes for Mobile WSN

The schemes already discussed for Static WSN is not effective for Mobile WSN. The detection in Mobile WSN for Node Replication Attack is classified into two categories (ie) Centralized and Distributed.

4.1 Detection Scheme in Mobile WSN for Centralized Approaches

In Mobile WSN for Centralized Approaches there is a monitor to control all the mobile nodes. The different detection scheme is discussed in Table 3.

4.1.1 SPRT

Ho et al.[10,11] proposed a detection scheme, SPRT (Sequential Probability Ratio Test) for mobile based WSN.

Table 3. Detection Scheme in Mobile WSN for Centralized Approaches

Detection Schemes	Communication Overhead	Storage Overhead
SPRT	O(√n)	O(1)
TDD	O(√n)	O(n)

n-no.of nodes

This method has a low error rate. In this method it measures depends upon the speed limit. If the speed limit is high then it is check for node id. If nodeid also same then assign it as replicated node.

4.1.2 TDD

Xing et al.[15] use time domain method and space domain method for detecting the clone nodes. In this method one-way hash function is used. SDD scheme use only localized scheme that produces low communication overhead. This scheme use one-way hash.

4.2 Detection Scheme in Mobile WSN for Distributed Approaches

In Mobile WSN for Distributed Approaches there are different detection scheme is discussed and shown in Table 4.

4.2.1 XED

Yu et al.[12] proposed Extremely Efficient Detection. If a sensor node meets the other node then both the node shares the random number. Again, if it meets the same node again it checks by verifying the random number. If two nodes are in the communication range they first generate random number of bits. Each node should manage the table to store the node ID and random number which is generated. Again, if it meets the node, then it compares with the random number. If the random number is same then a new random number is generated by the two nodes. XED technique can easily identify the replica node, but its increase the memory capacity.

4.2.2 EDD (Efficient and Distributed Detection)

Yu et al.[13] proposed an EDD scheme with two methods, offline step and online step. In offline step, deployment of the sensor nodes is done by network planner. The online step is used by each node for detecting the clone nodes by comparing with the number of encounters at some fixed

Table 4. Detection Scheme in Mobile WSN for Distributed Approach.

Detection Schemes	Communication Overhead	Storage Overhead
XED	O(1)	O(n)
EDD	O(1)	O(1)
Unary Time Location Storage and Exchange	O(n)	O(√n)
Multi time	O(n)	O(√n)
SEDD	O(n)	O(ξ)
Mobility Assisted Distributed	O(n log n)	
SDD-LC	O(1)	O(n)
SDD-LWC	O(d)	O(n)
Localized Algorithm	O(1)	O(1)

n – No. of nodes in the network, d – Degree of neighboring nodes, g - no. of witness nodes, r - Communication radius, rc – No of neighboring nodes forwards location claims, *s* - The number of sensors in a cell, *M* - the number of rows in the superimposed, ξ – Distinct IDs from set of nodes as monitorset, d - number of nodes randomly check for paradox check.

time interval. This scheme is not applicable in large-scale WSNs.

4.2.3 Unary Time Location Storage and Exchange (UTLSE)

Deng et al.[14] proposed UTLSE (Unary Time Location Storage and Exchange) scheme which detects the replicas of each of the two witness nodes. It stores only the time-location claim.

4.2.4 Multi-Time-Location Storage & Diffusion (MTLSD)

Deng et al.[14] proposed a MTLSD protocol for storing time-location claims. The probability is greater than the UTLSE.

4.2.5 Storage-efficient EDD (SEDD) Scheme

Yu et al.[13] proposed a SEDD scheme. The main idea in this scheme is to monitor all nodes. Each node will monitor sub nodes in a particular time interval, which is called as monitor set. The storage overhead is also reduced.

4.2.6 Mobility Assisted Distributed

Deng et al.[14] proposed the distributed approach which has no routing information. If two mobile nodes meet each other then they exchange their time location claims. If a monitor node receives a time-location of its tracked neighbour node, but it does not transmit the time-location of the witness. If the witness is not in the range but it stores that location claim.

4.2.7 SDD-LC

Xing et al.[15] proposed a SDD-LC which is to exchange information for every mobile node is verified with the data stored in local memory.

4.2.8 SDD-LWC

Xing et al.[15] proposed a SDD-LWC. A common table is used for sharing the information between nodes.

4.2.9 Localization Algorithm

Chia et al[16] scheme is for securing and detecting the clone nodes. The main advantage is efficiency. This scheme is mainly for mobile nodes.

5. Conclusion

Detecting node replication attack is a very important issue in sensor networks. This paper reviews about the schemes which is discussed by the researchers for detecting node replication attack. The various detecting scheme is classified it into two types: distributed and centralized. For both the centralized and distributed schemes the memory, communication cost overhead and detection rate is discussed.

6. References

1. Brooks R, Govindaraju PY, Pirretti M, Vijaykrishnan N, KandemirMT. On the detection of clones in sensor networks using random key predistribution. IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews. 2007 Nov; 37(6):1246–58.
2. Choi H, Zhu S, La Porta TF. SET: Detecting node clones in sensor networks. Third International Conference on Security and Privacy in Communications Networks; 2007. p. 17–21.
3. Yu CM, Lu CS, Kuo SY. CSI: Compressed sensing-based clone identification in sensor networks. IEEE International Conference on Pervasive Computing and Communications; 2012 Mar. p. 290–5.
4. Xing K, Cheng X, Liu F, Du DHC. Real-time detection of clone attacks in wireless sensor networks. International Conference on Distributed Computing Systems; 2008 Jun. p. 3–10.

5. Znaidi M, Ubeda MS. Hierarchical node replication attacks detection in wireless sensors networks. Proceedings of IEEE Personal, Indoor and Mobile Radio Communications; 2009 Sep 13-16; Tokyot. p. 82–6.
6. Parno B, Perrig A, Gligor V. Distributed detection of node replication attacks in sensornetworks. Proceedings of IEEE Symposium on Security and Privacy; 2005 May 8-11. p. 49–63.
7. Zhu B, Addada VGK, Setia S, Jajodia S, Roy S. Efficient distributed detection of node replication attacks in sensor networks. Twenty-Third Annual Conference in Computer Security Applications; 2007 Dec. p. 257–67.
8. Conti M, Di Pietro R, Mancini LV, Mei A. A randomized, efficient and distributed protocol for the detection of node replication attacks in wireless sensor networks. Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing; 2007. p. 80–9.
9. Zeng Y, Cao J, Zhang S, Guo S, Xie L. Random walk based approach to detect clone attacks in wireless sensor networks. IEEE Journal on Selected Areas in Communications. 2010 Jun; 28(5):677–91.
10. Ho JW, Wright M, Das SK. Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing. IEEE Transactions on Mobile Computing. 2011 Jun; 10(6):767–82.
11. Ho JW, Wright M, Das SK. Fast detection of replica node attacks in mobile sensor networks using sequential analysis. Proceedings of the IEEE INFOCOM; 2009 Apr 19-25; Rio de Janeiro. p. 1773–81.
12. Yu CM, Lu CS, Kuo SY. Mobile sensor network resilient against node replication attacks. Proceedings of IEEE Communications on Sensor, Mesh and Ad Hoc Communications and Networks; 2008 Jun 16-20; San Francisco, CA. p. 597–9.
13. Yu CM, Lu CS, Kuo SY. Efficient and distributed detection of node replication attacks in mobile sensor networks. Proceedings of the 70th IEEE Vehicular Technology. 2009 Sep 20-23; Anchorage, AK. p. 1-5.
14. Deng X, Xiong Y, Chen D. Mobility-assisted detection of the replication attacks in mobile wireless sensor networks. Proceedings of 6th Annual IEEE International Conference on Wireless and Mobile Computing, Networking and Communications; 2010 Oct 11-13. p. 225–32.
15. Xing K, Cheng X. From time domain to space domain: Detecting replica attacks in mobile ad hoc networks. Proceedings of IEEE International Conference on Computer Communications; 2010 Mar 14-19. p. 1–9.
16. Yu C-M, Tsou Y-T, Lu C-S, Kuo SY. Localized algorithms for detection of node replication attacks in mobile sensor network. IEEE Transactions on Information Forensics and Security. 2013 May; 8(5):754–68.