ISSN: 0974-6471, Vol. 10, No. (3) 2017, Pg. 653-659

Oriental Journal of Computer Science and Technology

Journal Website: www.computerscijournal.org

Analysis of Clone Detection Approaches in Static Wireless Sensor Networks

SACHIN LALAR, SHASHI BHUSHAN and SURENDER

[1]Ph.D. Research Scholar, CSE, IKGPTU, Kapurthala, India.
[2]Professor, I.T. CGC, Landran, Punjab, India.
[3]A.P., Computer Appl. GTB, Bhawanigarh, India.

Abstract

Wireless Sensor Networks (WSNs) are developing very fast in the wireless networks. The wireless sensor network has the characteristics of limited memory, small size and limited battery. WSNs are vulnerable to the different types of attacks due to its characteristics. One of the attacks is clone node attack in which attacker capture the nodes from the network and stoles the information from it and replicates it in the network. From the clone nodes, the attacker can easily launch the different type of attacks in the network. To detect the clone node, different methods has been implemented .Each method having advantages and limitations. In the this paper, we explain the different methods to detect the clone nodes in the static wireless sensor network and compare their performance based on the communication cost and memory.

Article History

Received: 21 July 2017
Accepted:08 August 2017

Keywords

WSN,
Clone attack,
Clone attack detection,
Centralized approach,
Distributed approach.

Introduction

The Wireless Sensor Network (WSN) is a collection of wireless sensor nodes which is small in size. WSN consists with base station which can communicate with sensor nodes by using radio link. Data is collected at the wireless sensor node, compressed and transmitted to the base station at once[1]. WSN may be deployed in harsh surroundings to complete the military and common tasks[2]. WSNs are vulnerable to the different types of attacks due to its characteristics. Different attacks on WSN are Selective forwarding attack, Acknowledgement spoofing ,Sinkhole, Wormholes, Sybil, HELLO flood, Sniffing attack, Data integrity attack, Energy drain attack , Black hole attack, Denial of service, Physical attacks, Traffic analysis assault and clone Attacks[3]. One of the attacks is clone node attack in which attacker capture the nodes in the network and stoles the information from it and replicates it in the network. From the clone nodes, the attacker can easily launch the different type of attacks in the network[4].

The main purpose of this paper to describe the different clone detection approaches in wireless sensor network. The rest of this paper is organized

CONTACT Sachin Lalar sachin509@gmail.com Ph.D. Research Scholar, CSE, IKGPTU, Kapurthala, India.

To link to this article: http://dx.doi.org/10.13005/ojcst/10.03.14

as follows. Section 2 describes about clone Attack. In section 3, we have discussed clone attack detection methods. In section 4, we summarize the existing Centralized and distributed detection protocols used to detect clone nodes in static sensor networks. We present a comparison between these protocols in section 5.

Clone Node Attack

To launch the clone node attacks, first the attacker captures the one or few of legitimate nodes from the network then attacker clones or replicates them in the network by using the secret information from the captured node. The attacker can easily launch the different type of attacks from the clone node and can decrease the performance of the network. The following are the causes of clone node attack:

- It creates an in depth damage to the community due to the fact the replicated node also has the same identity because the legitimate member.
- It creates numerous assaults by means of extracting all the mystery credentials of the captured node.
- It corrupts the monitoring operations by means of injecting false records.
- It can cause jamming in the network, disrupts the operations in the community and also initiates the Denial of Service (DoS) assaults too.
- It is hard to detect replicated node and consequently authentication is hard[5].

Clone Attack Detection

There are two types of wireless sensor networks: Static and Mobile. In static wireless sensor networks, the sensor nodes do not change their position after randomly deployment. The positions of sensor nodes are static in nature. In the second type (Mobile Wireless Sensor Network), the sensor nodes can change their position as per the requirement. So the sensor nodes are mobile in nature. There are different methods in static and mobile wireless sensor network to detect the clone node attacks. In the static WSN, there are two types of method to detect the clone nodes: Centralized and Distributed.

In a centralized method to detect the clone node, when a new sensor node wants to join the network, it first publicizes the message, which containing its location and identity, to the neighbors. The neighbors forward its location to the base station. With vicinity information from the nodes in the networks, the base station will find out the node which claims more than one location. If any node find out then the base node will broadcast the message in the network about the node and then that clone node will revoke from the network. The centralized method is easy but there are some drawbacks in this method. If base stations fail then the detection approach is also fails. If base station is compromised or blocked by attacker then attacker can upload any variety of replicas inside the network. The message/transmission cost is high in this method as all nodes broadcast the message towards the base station[5].

The second method for detection of clone node is Distributed method in which detection of clone node is distributed among nodes. So the drawback of the centralized method is overcome by the distributed method. When a new node wants to join the network, its region claim is forwarded to the corresponding witness nodes. If any witness node gets two one-of-a-kind location claims for the identical node ID, then the position of clone node is detected[6].

Clone Attack Detection In Static Sensor Nodes

Centralized approach

There are following centralized method for detecting the clone nodes as:-

Straight forward Scheme

In this method, when a new sensor node wants to join the network, it first publicizes the message, which containing its location and identity, to the neighbors. The neighbors forward its location to the base station. With vicinity information from the nodes in the networks, the base station will find out the node which claims more than one location. If any node find out then the base node will broadcast the message in the network about the node and then that clone node will revoke from the network.

The centralized method is easy but there are some drawbacks in this method. If base stations fail then the detection approach is also fails. If base station is compromised or blocked by attacker then attacker can upload any variety of replicas inside the network. The message cost is high in this method as all nodes broadcast the message towards the base station[5].

SET Protocol

SET scheme is a centralized approach in which sub region are consisting by dividing the network. The network is divided such that node having one hop in the sub region. An elected node becomes a leader from a sub region. A tree is built up in such a way base station of the network become the root of it and leader become the node of the tree. To detect the clone node, the leader will send the identity of all the nodes from its sub region to its parent of tree. Then the parent node execute the intersection function of set on data receive from its child. If any non empty result comes then the clone node is detected and result is sent to the root node. Otherwise it forwards all information to its parent of tree[7].

Pair wise Key Distribution

In this method, each node of the network is preloaded with random keys. These keys are used by node with certain pattern. The base station checks the key of each node when it receives the data from the nodes. It can detect the clone key by analyzing the authentication statics of the node[8].

Real Time Detection protocol

In this method, each node calculates its fingerprint based on S-disjoint code which is preloaded in each sensor node. After that node also calculate its neighbor fingerprint. The base station also computes the fingerprint of each node of the network. The node sends the data along with its finger print to the base station. The base station verifies the finger print of the node. Any false fingerprint of the node detected as clone node by the base station[9].

Distributed approach

There are following distributed method for detecting the clone nodes in the static wireless sensor network.

Broadcast Protocol

This is a simple approach in which every node of the network broadcast its location with all its neighbors' ids. When any node gets this message, it will check the list with its neighbors. If any matching find, that clone node is revoked from the network[10].

Deterministic Multicast (DM) Protocol

This method uses the claimer-reporter-witness approach. The node is called claimer when it broadcast its identity with its neighbor' ids. The reporters which perform the mapping function on claimer id. The neighbor of claimer sends its claim to the node called witness. If witness node obtains two different location claim of same node then clone node is detected[11].

Randomized Multicast (RM) Protocol

It is probabilistic algorithm which uses the claimer-reporter-witness approach. In this method, the node location claim is randomly distributed among selected set of witness which is based on combination theory. If a node receives more than one claims of the same node with dissimilar locations, it uses these conflicting claims as indication for the node replication[12].

Line Selected Multicast (LSM) Protocol

This method is similar to the RM method. The only difference between the RM and LSM is that LSM method forwards the location claim to addition witness node which is selected on base of routing topology. Clone node is detected through the intersection of paths generated of nodes with two unique node claims of equal ID and coming from distinct nodes[13].

Localized multicast

Single Deterministic Cell (SDC)

SDC method is based on localized multicast and variation of DM method. In this method, network is divided into small cells. The location claim of the node is sent to its cells reporter. The node pronounces its locality to each neighbor, which first checks the validity of the signature of the claimer. Then each neighbor decides itself whether forwards the request to witness or not. If a neighbor wants to forward the request then it executes a geographic hash function to decide the destination location.

When the witness gets a location declare with the equal identification but a specific area compared to a formerly saved declares, it forwards each location claims to the base station. The base station revokes the clone nodes from the network by broadcasting the message.

Parallel Multiple Probabilistic Cells (P-MPC)
This method is similar to the SDC. In this method, the claimer message is forward to multiple deterministic cell reporters. When a node declares its location, each neighbor independently makes a decision whether to forward the request or not in the same manner as in SDC scheme[14].

Randomized Efficient and Distributed (RED) Protocol
This method is combination of DM and RM. The location claim of the node is sent to its cells reporter. The node pronounces its locality to each neighbor, which first checks the validity of the signature of the claimer. The witness node checks the request based on a pseudo random function of node's ID. Location claims with the equal node ID will be moved forward to identical witness nodes in the each detection section[15].

Memory Efficient Multicast Protocols
Memory Efficient Multicast using Bloom filters (B-MEM)
In this method, claimer request is randomly forwarded on a line segments. All the halfway nodes in the path serve as watchers even as the primary and ultimate node function witnesses. When the node receives the region claim, it plays the 2-section conflict check to discover warfare claims.

Memory Efficient Multicast using Bloom filters and Cell forwarding (BC- MEM)
In this method, the network region is split into virtual cells. An anchor point is assigned for every node in each cell. The node close by to the anchor factor is referred to as anchor node. The claimer request forwarded to the anchor factor of the respective cell. The message transmitted from one anchor node to every other till it reaches on the last mobile[16].

Hierarchical Distributed Algorithm (HDA)
This method works in three steps. In first step, Clusters are consisting by dividing the network. The network is divided such that node having one hop in the sub region. An elected node becomes a cluster head in a cluster. A tree is built up in such a way base station of the network become the root of it and cluster head become the node of the tree. Each transmission of the message is done through this tree. The clone node detection is completed by the cluster nodes by using of a Bloom filter mechanism[17].

Random Walk Based Protocols
Random Walk (RAWL)
In the RAWL, each node publicizes a signed area claim. The neighbors of claimer probabilistically transmit the claim to randomly selected nodes. Each randomly selected node transmits the message containing the claim to start a random walk inside the community. If any witness gets specific location claims for a identical node ID. This will bring the detection of the cloned node.

Table Assisted Random walk (TRAWL)
In this method, when a randomly selected node begins a random walk, all the surpassed nodes will nonetheless become witness nodes. They do now not surely save the place claim, as an alternative, they save the place declare independently. When receiving vicinity claim of a node will first discover the entries that have the same node ID in its table. Then if any entry is located, the node will compute the digest of the claim and evaluate the digest. When digest are specific, the node detects a replicate node[18].

Detection of Node Capture Attack (DNCA)
This method uses the idea that the bodily captured nodes aren't contributed inside the community from the captured duration to the redeployment period. The captured nodes no longer take part in any community operation during this era. This method measures the absence term of a sensor node and compares it to a predefined threshold. If it is more than to the threshold value, the sensor node taken into consideration as a captured node[19].

Cell based Identification of Node Replication Attack (CINORA)
The network is divided into geographical cells similar to the cellular network. The location claimer of the node is dispensed among the subset of

cells to stumble on any replication. These cells are execute the intersection function of set on data receive from its child. If any non empty result comes then the clone node is detected and result is sent to the base station[20].

Comparision Of Protocols

In this section, we will compare all the protocols of clone detection according to the type, type of approach, Computation overhead and type of scheme used. The Table 1 shows the comparison of the protocols. Table 2 represents communication costs and communication costs of various clone node detection protocols.

From the tables, we find out that SDC protocol has the low communication value than other protocols and RED protocol has the minimum communication overhead for large community. The SDC protocol has decrease memory overhead than other protocols. The RED and BC-MEM protocols have better detection probability than other protocols. The P-MPC protocol has greater resilience in opposition to node compromise than other protocols.

Table 1: Comparison of Protocols

No	Protocol	WSN Type	Type of approach used	Computation Overhead	Type of Scheme used
1	SET	Static	Centralized	High	Base station based
2	Real Time	Static	Centralized	High	Neighbour based
3	Pair wise Key Distribution	Static	Centralized	High	Group based
4	Straightforward Scheme	Static	Centralized	High	Base station based
5	Broadcast	Static	Distributed	Comparably Low	Network broadcast
6	DM	Static	Distributed	Average	Witness based
7	RED	Static	Distributed	Low	Witness based
8	RM	Static	Distributed	Low	Witness based
9	LSM	Static	Distributed	Comparably High	Witness based
10	SDC	Static	Distributed	Low	Witness based
11	P-MPC	Static	Distributed	Low	Witness based
12	B-MEM	Static	Distributed	High	Witness based
13	BC-MEM	Static	Distributed	High	Witness based
14	HDA	Static	Distributed	High	Cluster based
15	RAWL	Static	Distributed	Average	Witness based
16	TRAWL	Static	Distributed	Average	Witness based
17	DNCA	Static	Distributed	High	Base station based
18	CINORA	Static	Distributed	High	Group based

Table 2: Communication Cost & Memory Cost

Protocol	Communication cost	Memory Cost
SET	O(n)	—-
Pair wise Key Distribution	O(“n)	O(1)
Broadcast	$O(n^2)$	O(d)
DM	O(gln.g”n/d)	O(g)
RED	O(r.”n)	O(r)
RM	$O(n^2)$	O(“n)
LSM	O(n”n)	O(“n)
SDC	O(r.”n)+O(s)	W
P-MPC	O(r.”n)+O(s)	W
B-MEM	O(kn”n)	O(tk+tk”n)
HAD	$O(N^2)$	O(N)
RAWL	O(“nlogn)	O(“nlogn)
TRAWL	O(“nlogn)	$O(1)^2$
DNCA	O(n “n)	O(n)

Conclusions

In this paper, we have discussed the various methods to detect the clone attacks in static WSN. Wireless sensor networks are deployed in adverse environment and susceptible to numerous types of attacks. In static centralized protocols, Real Time protocol has the lowest verbal exchange overhead than other protocols. In static distributed protocols, we discover that SDC protocol has decrease communication value than other protocols for smaller size community and RED protocol has the bottom communication overhead for large community. The SDC protocol has decrease memory overhead than other protocols. The future work will be implementation of these methods and compare the result in the simulator.

References

1 Yong Wang,Garhan Attebury and Byrav Ramamurthy "A survey of security networks issues in wireless sensor networks"IEEEcommunicationsSuveysandTutorials,vol.*8*.no. 2,2006.

2 Ian F.Akyildiz, William Su, Yogis S.Subramaniam and Real Cayirci, "A survey on sensor network", IEEE Communications Magazine, pp 102-114, August 2002.

3 Cris Townsend, Stevan Arms, "Wireless sensor network: principles and applications", Chapter 22, pp439-449.

4 Yan-Xiao Li, Lain-Qin, Ian-Liang, "Research on wireless Sensor network security", IEEE Computer Society, International Conference on Computational Intelligence and Security, 2010.

5 M.Conti, R.DiPietro, L.V.Mancini, A.Mei, "Requirements and open issues in distributed detection of node identity replicas in WSN" ,in SMC'06, 2006, pp.1468–1473.

6 J.W.Ho,"Distributed detection of node capture attack in wireless sensor networks", in smart wireless sensor networks, pages 345-360, 2010

7 H.Choi, S.Zhu, T.F.LaPorta, "SET : Detecting node clones in sensor networks" , *in:SecureComm'**07**, 2007, pp.341–350.*

8 Jun-Won Ho, Dogging Lin, Matthew Wright, SajaiK.Das "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks", Preprint submitted Elsevier, March 2009.

9 Kai Xing,Fang Liu,Xiuzhen Cheng,David H.C.Du," Real-time Detection of clone attacks in Wireless Sensor Networks",IEEE ICDCS 2008

10 B.Parno, A.Perrig, V.D.Gligor, "Distributed detection of node replication attacks in sensor networks" , *in:S&P'05, 2005, pp.49–63.*

11 Bio Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia, Sushil Jajodia and Sankaradas Roy, "Efficient Distributed Detection of Node Replication Attacks in sensor Networks",IEEE Computer Society, 23 rd Annual Computer Security Applications Conference,Pages 257 – 266, 2007

12 C. Bekara and M. Laurent- Maknavicius,"A New Protocol for securing Wireless Sensor Networks against nodes replication attacks"Third IEEE International Conference on Security and Privacy in communication networks,2008

13 Bryan Parno, Adrian Perrig, Virgil Gligor, " Distributed Detection of Node Replication Attacks in Sensor Networks ", In proceeding of the IEEE Symposium on Security and Privacy , 2005

14 Mauro Conti, Roberto Di Pieto, L.V.Mancini and A.Mei,"A Randomized and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks ", Proc. ACM MobiHoc, Pages 80-89, Sept 2007

15 Bio Zhu, Sanjeev Setia, Sushil Jajodia, Sankardas Roy and Lingyu Wang "Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks", IEEE Transactions on Mobile Computing, Vo1 9, No 7, Pages 913-926, July 2010

16 Bio Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia, Sushil Jajodia and Sankaradas Roy, "Efficient Distributed Detection of Node Replication Attacks in sensor Networks",IEEE Computer Society, 23 rd Annual Computer Security Applications

Conference,Pages 257 – 266, 2007

17 Wassim Znaidi, Marine Minjer, Stephane Uheda,"Hierachical Node Replization Attacks Detection in Wireless Sensors networks "IEEE, Pages 82-86, 2009.

18 Yingpei Zeng, Jiannong Cao, Shigeng Zhang,Shanqing Gao 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 Pages 677-691, June 2010

19 Ming Zhang, Vishal Khanapure, Shigang Chen,Xuelian Xiao, "Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Network" IEEE Pages 284-293, 2009

20 Y.Lou,Y.Zhang and S,Liu,"Single hop detection of node clone attacks in mobile wireless sensor networks", in Proceedings of the International Workshop on Information and Electronics Engineering (IWIEE)2012.