Detection of Clone Attacks in WSNs – A Survey

C. Geetha[1], Dr.M. Ramakrishnan[2]

[1]Department of CSE
R.M.K. Engineering College, Chennai, TN, India

[2]Department of IT
Velammal Engineering College, Chennai, TN, India

ABSTRACT -- ***A wireless sensor network is a collection of nodes organized in to a cooperative network. This network is prone to various attacks due to poor security. One of the attacks is clone attack in which an adversary captures some nodes and replicates them including the cryptographic in formation and deploys them in the network. Several algorithms are developed to detect clone attacks, in static WSNs and mobile WSNs. Each one has its own advantages and disadvantages. This paper surveys these algorithms and compares their performance based on parameters like communication cost and memory.***

Keywords - clone attack, witness node, sensor network

1. INTRODUCTION

Wireless sensor network, a network of sensor nodes, which are tiny with limited resources that communicate with each other to achieve a goal, through the wireless channels. This network is mainly used in military applications for monitoring security and in civil applications. This network is deployed in harsh and hostile environments. Based on operating nature, it is unattended and prone to various attacks. The basic security requirements of wireless sensor network are integrity, availability, confidentiality and communication.

Attacks in wireless sensor networks are classified into internal attacks and external attacks. In internal attacks, compromised nodes can steal secrets from encrypted data, can report wrong information, can report other nodes as compromised nodes and can breach routing by introducing many routing attacks. In external attacks, attackers can capture sensor nodes and reprogram them and can deploy nodes with larger computing resources such as laptops to attack sensor nodes.

Several attacks includes Denial of Service, attacks on information, Sybil attack, black hole attack, warm hole attack and clone attack[6][9]. One of the common attacks is clone attack or node replication attack, where an adversary node captures some nodes and makes duplicates of the original node including all cryptographic information and thus inserts these duplicates in the network. These duplicates use the same ID as the original node in the network. Thus it takes full control over the network. The consequence of this attack is injecting false data, modify the data, initiating a warm-whole attack, dropping packets, thus all these results in leaking of authorized data to an adversary. The simplest way of protecting clone attacks by an adversary node is that, extracts the secret key elements from an attacked node by using a technique called virtue of tamper-resistance hardware. But to implement this technique, the hardware based measures are too expensive in practical. Several algorithms were developed so far to detect clone attacks in both static and mobile sensor networks. The major requirements of all these algorithms are the witnesses and the communication overhead[1]. In this paper we do a study on these algorithms and analyze the performance in terms of detection ratio, speed, communication overhead (memory occupation) and energy consumption.

The remaining part of this paper is organized as follows: Section 2 describes the centralized algorithms and distributed algorithms, section 3 compares all these algorithms in terms of Communication overhead and memory usage and section 4 concludes the analysis.

2. DETECTION ALGORITHMS

Based on the detection methodologies, we classify the clone attack detection algorithms as [8][11]

1. Centralized algorithms for static WSNs
2. Centralized algorithms for mobile WSNs

3. Distributed algorithms for static WSNs
4. Distributed algorithms for mobile WSNs

Centralized clone detection algorithms relies on centralized node, may be a base station, where the location or information of all nodes were maintained. But this centralized approach is prone to single point of failure and communication overhead. Only the BS is involved in the detection of clones.

In Distributed clone detection algorithms, several nodes are involved in detecting clones. They distribute the location claims to several nodes which are randomly selected and called as witnesses.

2.1 Centralized algorithms for static WSNs

2.1.1 Preliminary Approach

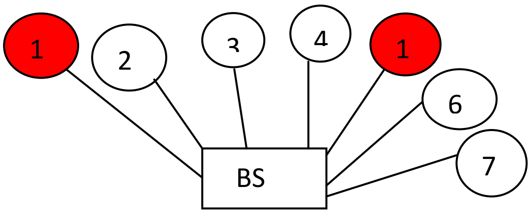
All the nodes send its neighbor's estimated location information and IDS to the base station. The BS compares the IDs and if two nodes with same ID and different location are received by BS, then it finds that there is a cloned node.

Disadvantage

- If the BS fails due to some hardware problem then it is difficult to detect the attacked clone.
- Less number of chances to detect the clone attacks.

Advantage

- The BS contains the ID and information location of all nodes in it.



Nodes with same id and different locations

Fig. 1 Clone attack

2.1.2 Random Key Predistribution

Each and every node is assigned a key to authenticate the nodes. Based on how often these keys are used by the nodes, the key is identified as cloned or not. Each node uses a Bloom filter to count the number of times the key is used. This filter is transferred to the BS, which will verify the count with the predefined threshold, the particular node is found to be a cloned node. But exactly this scheme finds the clone key not clone node.

Disadvantage: High false negative and positive rates.

2*.1.3 SET detection*

This is a method used widely, to detect the clones by using SET operations such as UNION, INTERSECTION of subset of Ids in a network. An intersection of two different subsets must always be empty. If there is a non-empty intersection then the BS revokes that the corresponding two nodes has been cloned.

All previous schemes are used in static WSNs. These schemes are not suitable for mobile WSNs. Because, in mobile WSNs, nodes change the locations often. There is a fact that mobile nodes can't move faster than the maximum configured speed of the network. If any node moves faster than the maximum speed, there must be more nodes with same identity available in the network.

2.1.4 SPRT

When the sensor node moves to a new location, the neighbors ask for the location claim and time information that will be sent to the BS[13]. The BS determines the speed from two consecutive claims and if the speed exceeds the maximum configured speed of network, it found that the mobile node has been replicated. It is the best mechanism in terms of number of observations to reach the decision process. A method in centralized using SPRT, probably a type of SPRT called BIASED-SPRT[15].

SPRT based node compromise detection and revolution schema will not work fast and accurately if more than 50% of the nodes n each zone are compromised under reasonable configuration. So in order to enhance the SPRT based scheme against the false zone-trust report attack with a large no of compromised nodes the same introduced in the biased-SPRT.

In this Biased-SPRT sampling strategy is modified .In that the SPRT takes the sampling leads to acceptance of the H_0 (high trust sample) with the less weight than the ones leading to acceptance of H_1 (low trust samples) ensuring that the false positive rate remains below the desired rate. This modification is called as biased sampling and the corresponding scheme is called as Biased-SPRT.

High trust sample is less likely to be accepted than a low-trust sample if the zone is in un-trust worthy. In accepting the null hypothesis and greater false positive rates biased sampling results in greater delay, but while designing the system these are not major costs.

Even if the compromised node is more than 50% then also the biased sampling improves the resilience of the proposed scheme against the false zone-trust report attack.

Performance analysis

The same communication, computation and storage overheads required for biased-SPRT is same as the SPRT because it only changes the sampling strategy of the SPRT and thus does not affect these overheads. However, the change in the sampling strategy affects the average number of samples and attestation overhead of the SPRT.

2.2 Centralized algorithms for mobile WSNs

2.2.1 Fast Detection – SPRT

SPRT is one dimensional random walk with lower and upper limits. Before random walk, null and alternate hypothesis are defined. Null is associated with lower limit and alternate is associated with upper limit[7].

Each time a mobile sensor node moves to a new location, a signed claim containing its location and time information are send to the neighbors. These neighbors forward the message to BS. The base station computes the speed from every two consecutive claims of a mobile node and performs the SPRT. If the maximum speed is exceeded by the mobile node, set the alternate hypothesis to indicate cloned node.

2.3 Distributed Algorithms for static WSNs

2.3.1 Using Fingerprint (Real-time Detection)

The clones are detected using a fingerprint that includes information of neighboring nodes. Since the fingerprints are fixed on a particular node, it requires additional complex process to add new sensor nodes[10].

Advantages

- When compared to security, this protocol achieves 100% detection of all clones that are attacked assuming that all the messages successfully reach the base station.

2.3.2 Node-to-network delivery

Node to network broadcast is used. Every node collects the IDs and location of its neighboring nodes. When a node receives a broadcast message from the others, the node compares the other neighboring node with its own neighbors, if there is a collision of IDs in the two neighboring nodes of distinct locations, and then the corresponding nodes are cloned and revoked[14].

Advantage

- The distributed methods are more effective than the centralized schemes.
- Failure of the BS node does not cause any problems to the entire system.

Disadvantage:

- High communication overload in the network.

2.3.3 Determined Multicast

To reduce the communication cost, this scheme sends the location information to only a subset of nodes. When a node broadcasts its location claim to all neighbors, and these neighbors in turn send only to limited set of nodes which are called as witnesses. These witnesses are selected based on the function of node ID. If there is a replicated node, any one of this witness may receive the different location claims with same ID and it revokes the replicated node.

2.3.4 Detection using Group Deployment

We define the deployment zone of a group with radius R. Every node discovers its real location. If this node resides outside its home zone, it produces a signed claim by using its private key. Now every node discovers a set of neighbors and asks for authenticated location claim. If the distance between the node and its neighbor is larger than the communication range then neighbor will be removed from the list. Then it checks the distance between the neighbor and the deployment point is less than R (radius of the group), neighbor is marked as trusted, otherwise mark it as un-trusted[17].

The node forwards regular messages from its un-trusted neighbor, if it has received and verified the location claim, to the deployment point where all will get the claim message. If any nodes receive conflicting claims, then found that the neighbor node gets replicated.

2.3.5 Randomized Multicast

Same as the previous approach, but the neighbors probabilistically send the location information to randomly selected witnesses. If there is a replicated node, any one of this witness may receive the different location claims with same ID and it revokes the replicated node[4].

Advantage**:**

- Detects the replication with high probability using relatively limited number of witnesses[16].

2.3.6 Line Selected Multicast

This scheme uses the routing topology to detect the clones. In addition to the witness nodes, the intermediate nodes within the path can check for clones. Each node forwards the claims also saves the claims. For example, a node *a* and clone *a*' in the network. Neighbor of *a* sends the location claim to r witnesses. Each node stores this information also. When this information is transferred, on the path any node *w* verifies the signature on the claim and checks for the conflict with the location information on its buffer. If there is a conflict revokes the cloned node. Otherwise store the claim and forwards to the next node[5][12].

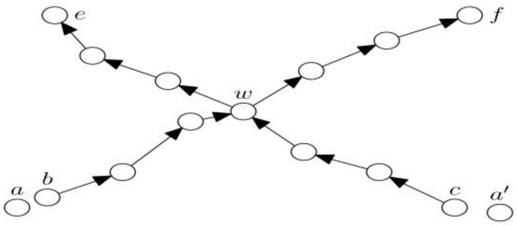


Fig. 2 LSM Approach

Advantage:

- Less communication cost
- High detection rate
- Less storage requirements.

2.3.7 RED

RED is similar, to the RM protocol but with witnesses chosen pseudo-randomly based on a network-wide seed. A random value, rand, is shared among all the nodes. This random value can be broadcasted with centralized mechanism. Each node digitally signs and locally broadcasts its claim—ID and geographic location. Each of the neighbors sends (with probability p) the claim to a set of g >= 1 pseudo-randomly selected network locations[3].

2.3.8 Agent Based Detection

Every node A prepares a signed location claim. The mobile agent gets the signed claim which is visited by it. The nodes information matrix is acquired through mobile agent routing algorithm. Each node A gets the information matrix verifies the signature and checks the distance between the neighbors and this cannot be bigger than the transmission range. When more than one entry for signed claim made in a single cell of an information matrix of one node, revokes the procedure for replicas[2].

2.4. Distributed algorithms for mobile WSNs

2.4.1. XED (eXtremely Efficient Detection)

Every sensor node is having a random number generator. When a node encounter another node, they exchange the random numbers. Once again the same nodes meet, they verify the random numbers exchanged already. If no match, clone node found[18].

Advantage**:**

- Communication cost is constant.
- Location information is not required to detect the clone node.

Disadvantages**:**

- Vulnerable to smart attackers.

2.4.2. SDD

If a node ***a*** does not meet the node ***b*** within twice the specified interval Δ, then the node is removed from the network and clone node is found[19].

Advantages:

- Each node is considered as witness.

Disadvantages:

- High communication cost and Less detection ratio.

2.4.3. EDD (Efficient and Distributed Detection)

The algorithm has two phases. In the first phase, the interval Δ is calculated and in the second phase, the messages are exchanged to find the clone[20].

Disadvantages**:** Vulnerable to smart attackers

2.4.4. SEDD (Storage EDD)

A node monitors only a set of nodes and exchanges the messages within the set[20].

Advantages**:**

- Reduces the number of messages exchanged.

3. COMPARISON

Table 1 Communication cost and Memory

Protocol Name	**Communication Cost**	**Memory**
Preliminary Approach	O(n)	O(n)
SET	O(n)	O(d)
SPRT	O(n)	O(d)

Deterministic Multicast	$O(g \ln g\sqrt{n} / d)$	$O(g)$
RED	$O(r \sqrt{n})$	$O(r)$
Randomized Multicast	$O(n^2)$	$O(\sqrt{n})$
Line-Selected Multicast(LSM)	$O(n\sqrt{n})$	$O(\sqrt{n})$
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)/O(n)	O(N)

Where,

n- No .of nodes in the network, d- Degree of neighboring nodes, r- Communication radius.

4. CONCLUSIONS

In this paper a study of various clone detection approaches was done. The distributed approach is more efficient than the centralized one because of single point of failure. The selection of witnesses is different for the approaches discussed for static WSNs. When the mobility is added, the algorithms become more complex. In future, we had a plan to design a new approach based on RED and LSM protocols, which might meet the requirements of clone detection algorithms and also high detection ratio with less time and communication cost.

5. REFERENCES

[1] Mauro Conti, Roberto Di Pietro , Luigi V. Mancini, and Alessandro Mei, “Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN”, IEEE International Conference on Systems, Man and Cybernetics, 2006, Taiwan.

[2] D.Sheela , Srividhya .V.R, Vrushali , Amrithavarshini and Jayashubha J.” A Mobile Agent Based Security System of Wireless Sensor Networks against Cloning and Sink Hole Attacks”, ICCTAI'2012.

[3] Mauro Conti, Roberto Di Pietro , Luigi Vincenzo Mancini, and Alessandro Mei, “Distributed Detection of Clone Attacks in Wireless Sensor Networks”, IEEE Transactions On Dependable And Secure Computing, VOL. 8, NO. 5, 2011.

[4] Bryan Parno, Adrian Perrig, Virgil Gligor , “Distributed Detection of Node Replication Attacks in Sensor Networks”.

[5] Wen TaoZhu, JianyingZhou, RobertH. Deng, FengBao , “Detecting node replication attacks in wireless sensor networks: A survey”, Journal of Network and Computer Applications 35 (2012) 1022–1034.

[6] Dr. G. Padmavathi , D.Shanmugapriya ”A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks ” International Journal of Computer Science and Information Security,Vol.4 No. 1&2,2009.

[7] Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis.

[8] Kwantae Cho, Minbo Jo, Member , IEEE, Tackyoung Kwon, Hsiao - Hwa Chen, Fellow, IEEE ,and Dong Hoon Lee, Member, IEEE” Classification and Experimental Ana;ysis for Clone Detection Approaches in Wireless Sensor Networks” IEEE SYSTEM JOURNAL .

[9] TEODOR-GRIGORE LUPU , Vasile Parvan 2,300223, Timisoara, ” Main Types of Attacks in Wireless Sensor Networks ” Recent Advances in Signals and Systems.

[10] Kai Xing, Fang Liu Xiuzhen Cheng, David H. C .Du, ”Real-time Detection of Clone Attacks in Wireless Sensor Networks” The 28th International Conference on Distributed Computing Systems.

[11] V. Manjula, C. Chellappan “REPLICATION ATTACK MITIGATION FOR STATIC AND MOBILE WSN” International Journal; of Network Security&Its Application(IJNSA)Vol.3,No.2,March 2011.

[12] Bryan Parno, Adrian Perrig, Virgil Gligor , “Distributed Detection of Node Replication Attacks in Sensor Networks”.

[13] Jun-Won Ho, Matthew Wright, Member, IEEE, and Sajil K. Das , Senior Member, IEEE,” Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.10, NO.6,June 2011.

[14] V. Ram Prabha, P . Latha, “An Overview of Replica Node Detection Wireless Sensor Networks” International Conference on Recent Trends in Computational Methods, Communication and Controls(ICON3C 2012)Proceedings Published in International Journal of Computer Applications(IJCA).

[15] Jun- Won Ho, Member, IEEE Computer Society, Matthew Wright, Member, IEEE, and Sajal K. Das, Senior Member, IEEE” Zone-Trust :Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequentil Hypothesis Testing” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING,VOL.9,NO.4,JULY/AUGUST 2012.

[16] Tamara Bonaci, Phillip Lee, Linda Bushnell, Radha Poovendran” A convex optimization approach for clone detection in wireless sensor networks” Contents List available at Elseivere Science Direct.

[17] Jun-Won Ho, Matthew Wright, Donggang Liu, and Sajil K.Das ,” Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks ” Ad Hoc Networks 7(2009)-1476-1488.

[18] Mauro Conti et al,” Emergent Properties: Detection of the Node-capture Attack in Mobile Wireless Sensor Networks” WiSec’08, March 31–April 2, 2008, Alexandria, Virginia, USA.

[19] Chia-Mu Yu et al,” Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks” 2009 IEEE

[20] Chia-Mu Yu et al,” Mobile Sensor Network Resilient against Node Replication Attacks” 2008 IEEE