Paper ID: E&TC09

DETECTION OF CLONE ATTACKS IN WIRELESS SENSOR NETWORKS ON THE BASIS OF CLASSIFICATION AND EXPERIMENTAL ANALYSIS

Miss. Raisa M. Mulla
M.E student
J.J.Magdum College of Engineering
Shivaji University, Kolhapur
Mullaraisa23@gmail.com

Mrs. P.P. Belagali
Asso. Professor
J.J.Magdum College of Engineering
Shivaji University, Kolhapur
ppbelagali@rediffmail.com

Mr. Shivraj A. Patil
M.Tech student
Department of Technology
Shivaji university Kolhapur
shivrajpatil111@gmail.com

Abstract- This paper presents a broad study on the finding of replication node in wireless sensor networks. Consider a very simple and vital physical dose on WSN which is called node replication attack or clone attack. It is also recognized as distinctiveness attack. Some algorithms are established to detect clone attacks; in static WSNs and mobile WSNs. Everyone has its own advantages and disadvantages. This paper surveys these algorithms and compares their performance based on parameters.

Index Terms - wireless sensor networks, Clone attacks, Witness Node

I. INTRODUCTION

Wireless sensor networks (WSNs), and particularly their security issues, have received great attention recently in both academia and industry. Since tiny sensor nodes in WSNs have meagre resources for computation, communication, power, and storage, it is inspiring to provide efficient security functions and mechanisms for WSNs. Above all, since WSNs are frequently deployed in aggressive environments, sensor nodes can be captured and compromised easily by an adversary who may extract secret data from the captured nodes. After such a compromise, a clone attack can be launched by duplicating the captured nodes and injecting them sporadically over the networks such that the adversary can enlarge the bargained areas by employing the clones. The secret information, such as access keys, extracted from the captured nodes and still contained in clones, may allow the challenger to gain access to communication systems throughout WSNs. For instance, clones would be Authenticated as honest nodes in a key establishment scheme of WSNs in different locations, eventually taking over a local sector or an entire network to launch various attacks, such as corrupting data aggregation, injecting false data, and reducing packets selectively. Thus, it is essential to detect clone nodes promptly for minimizing their damages to WSNs.

The simplest apologetic measure against the clone attacks is to prevent an adversary from extracting secret key materials from captured nodes by benefit of tamper-resistant hardware. However, the hardware-based defensive measures are too expensive to be concrete for resource-restricted sensor nodes. Various kinds of software-based clone detection schemes have recently been offered for WSNs, considering many different types of network configuration, such as device types and deployment strategies. The restriction of software based clone detection schemes is undoubtedly that they are not generic, meaning that their performance and success may depend upon their preconfigured network settings. The selection criteria of clone detection schemes with favour to device types, detection methodologies, deployment strategies and detection ranges, and then classifies the existing schemes according to the proposed criteria

II. BACKGROUND

NODE REPLICATION ATTACK

Wireless sensor network, an adversary mostly actually captures only one or few of legitimate nodes, then clones or copies them fabricating those duplications having the same identity (ID) with the captured node, and finally deploys an unreliable number of clones throughout the network.

Roots of node replication attack are as follows:

1) It creates a broad damage to the network because the fake node also has the same identity as the legitimate member.
2) It creates various attacks by extracting all the secret credentials of the captured node.
3) It corrupts the monitoring operations by injecting false data.
4) It can cause jamming in the network, disrupts the operations in the network and also initiates the Denial of Service (DoS) attacks too.
5) It is hard to detect fake node and hence authentication is hard.

A WSN can be either stationary or mobile. In static wireless sensor networks (SWSNs), the sensor nodes are fixed or mobile; that is, the sensor nodes are deployed accidentally, and after deployment their positions can't change. On the other finger, in mobile wireless sensor networks (MWSNs), the sensor nodes can move on their own, and after deployment, appearing at different places at different times.

Detection Techniques

In the total working schematic, a taxonomy of clone detection schemes of WSNs, in which the selection criteria is defined. Mainly, we split the taxonomy according to device types, such as static and mobile WSNs.

There are four main steps

1) Define selection criteria
2) Compare all clone Detection Schemes (SCRW, SDRW, SDGW, SDGL, MCW & MDW)
3) Clone Detection Schemes
4) Simulation Parameter testing

& graph Selection criteria

In the total working schematic, a taxonomy of clone detection schemes of WSNs, in which the selection criteria is defined. Mainly, we split the taxonomy according to device types, such as static and mobile WSNs. In Fig. 1, the clone detection schemes of static WSNs are classified into four types-

A. SCRW (static, centralized, random uniform, and whole)
B. SDRW (static, distributed, random uniform, and whole (SDRW)
C. SDGW (static, distributed, grid, and whole)
D. SDGL (static, distributed, grid, and local)

According to their detection methods, deployment strategies, and detection ranges. In Fig.1, the clone detection schemes of mobile WSNs are classified into two types according to their detection methods and detection ranges-

A. MCW (mobile, centralized, and whole)
B. MDW (mobile, distributed, and whole)

III. Compare all clone Detection Schemes (SCRW, SDRW, SDGW, SDGL, MCW & MDW)

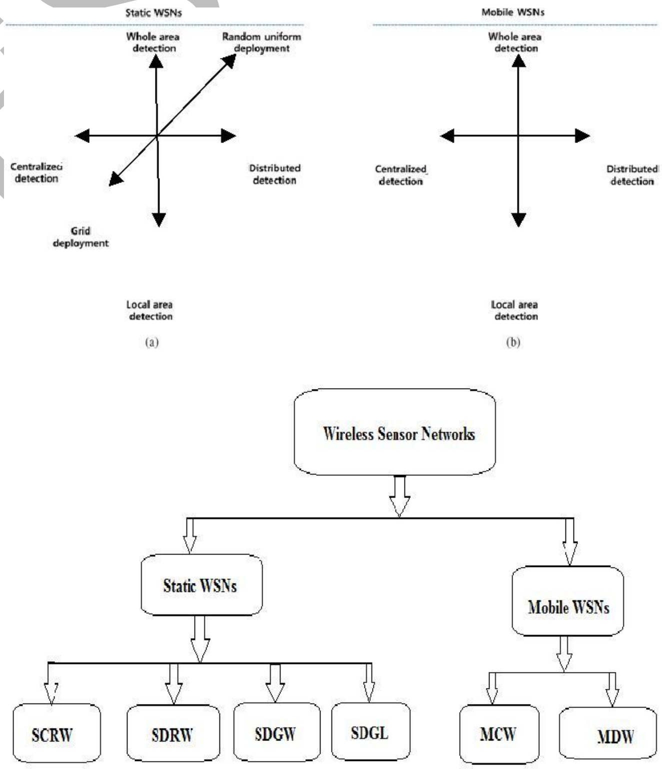

Fig.1. Classifications of WSNs detection procedures

IV. Detection Techniques for Stationary Wireless

To begin the design process of SHM first we need to understand the different components related to a structural health monitoring system and how they work and come together. A SHM system generally consists of the following modules, namely, array of sensors, data receiving, data transmitting system, data processing and control system, The array of sensors along with the data transmitting system are actual located on predetermined positions on the structure, whereas remaining systems arelocated on few meters away from bridge which can be used for monitoring and data analysis portion of SHM.

How it all works:

A. Type SCRW

In integrated techniques base station is measured to be a powerful central which is responsible for information merging and result making. During the detection process every node in the network sends its location claim (ID, Location Info) to base station (sink node) through its neighbouring nodes. Upon receiving the entire location claims, the base station forms the node Ids along their position, and if it finds two different locations with the same ID, it raises a clone node. SET: The network is accidentally distributed into exclusive subsets. Each of the subsets has a subset leader, and associates are one hop missing from their subset leader. Multiple roots are randomly decided to construct multiple sub trees, and each subset is a node of the sub tree. Each subset leader collects member information and forwards it to the root of the sub tree. The joining process is achieved on each root of the sub tree to detect replicated nodes. If the joining of all subsets of a sub tree is blank, there are no clone nodes in this sub tree. In the final stage, each root forwards its report to the base station (BS). The BS detects the clone nodes by computing the intersection of any two received sub trees. SET detects clone nodes by sending node information to the BS from subset leader to the root node of an accidentally created sub tree and then to the BS.

B. Type SDRW

In spread methods, no central consultant occurs, and special detection mechanism called claimer-reporter-witness is provided in which the discovery is made by locally distributed node sending the location claim not to the base station (sink) but to an accidentally designated node called witness node.

Deterministic Multicast (DM): DM protocol is a claimer-reporter-witness framework. The claimer is a node which locally broadcasts its position privilege to its neighbours, every neighbour helping as a reporter, and employs a function to map the claimer ID to an observer. Then the neighbour forwards the right to the observer, which will receive two different location claims for the similar node ID if the adversary has faked a node. One problem can occur that the adversary can also employ the purpose to identify about the observer for a given claimer ID, and may locate and compromise the witness node before the adversary supplements the copies into the WSN so as to evade the detection.

RM and LSM: The first protocol is called Randomized Multicast (RM) which distributes location claims to a randomly selected group of observer nodes. The another protocol, Line-Selected Multicast (LSM), exploits the routing topology of the network to select observers for a node position and consumes geometric probability to detect replicated nodes. In RM, each node broadcasts a location claim to its one-hop neighbours. Then, each neighbour selects randomly witness nodes within its message variety and forwards the position right with a probability to the nodes closest to chosen locations by using topological direction-finding. At least one observer node is possible to receive conflicting location claims according to birthday paradox when fake nodes exist in the network. In LSM, the main objective is to reduce the communication costs and raise the probability of discovery. Besides storing location claims in accidentally selected witness nodes, the middle nodes for furthering location rights can also be witness nodes. This seems like randomly drawing a line across the network and the joining of two lines becomes the evidence node of receiving conflicting position rights.

RED: Randomized, Efficient, and Distributed protocol called RED, for the finding of node duplication attack. It is executed at static intervals of time and consists in two steps. In first step, a random value is shared between all the nodes through base station. The second stage is called detection phase. In the detection stage, each node broadcasts its right (ID and location) to its neighbouring nodes. Each neighbour node that hears a right sends (with probability this right to a set of pseudo randomly selected network locations. The pseudo random function takes as an input ID, random number, and. Each node in the track (from claiming node to the witness destination) provides the message to its neighbour nearest to the destination. Hence, the fake nodes will be detected in each detection stage. When next time the RED executes, the observer nodes will be different since the random value which is broadcasted by the BS is changed.

Localized Multicast: Two distributed protocols for detecting node duplication occurrences called Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC). In both protocols, the entire sensor network is shared into cells to form a geographic network. In SDC, every node ID is uniquely mapped to one of the cells in the grid. When executing detection procedure, each node broadcasts a position claim to its neighbours. Then, each neighbour forwards the position claim with a probability to a unique cell by performing a geographic hash function with the input of node ID. Once any node in the destination cell receives the position right, it floods thelocation right to the entire cell. Each node in the destination cell stores the location right with a probability. Therefore, the clone nodes will be noticed with a certain probability since the position claims of clone nodes will be forwarded to the same cell. Like SDC, in the P-MPC structure, a geographic hash function is employed to map node distinctiveness to the destination cells.

C. Type SDGW

Proposed two grid-based clone detection arrangements, i.e., single deterministic cell (SDC) and parallel multiple probabilistic cells (P-MPC), which increase the accident probability of RM by using network information given to all node. In SDC, the IDs and positions of the neighbours are forwarded to a single zone that is resolute from single-way hash function with a node ID as input. However, in P-MPC, the pair information is forwarded to multiple zones that are resolute in the similar way. Then, every node checks whether or not the IDs received from the other nodes are in fight. Although P-MPC needs an advanced communication cost than SDC, it can detect clones by virtue of nodes in the extra zones, even in the case where altogether nodes in a given zone are compromised by an adversary.

D. Type SDGL

A specific network configuration based on grid deployment is preferred for local network clone discovery. A WSN organized by grid deployment can place sensor nodes in a predetermined zone and utilize their locations to sense clones. For instance, if a node is sensed in a zone that is far from its predetermined zone over a threshold distance, then it is suspected as a replicated node. This approach is a basic approach of local network clone detection. However the basic approach is effective, its discovery quality depends very much on a possible deployment error in WSNs. If honest node is situated erroneously in a zone that is out of the threshold distance, then the basic approach may produce a detection error (a false alarm) by determining it as a clone.

E. Type MCW

Mobile Centralized Techniques proposed a centralized detection scheme for mobile WSNs by exploiting the fact that a genuine node never travels outside the extreme speed. Every node in WSNs collects the IDs and locations of its neighbours along with their communication times, 3 and every node then transmits the composed data to the BS in reliable way. If a node moving over the maximum speed is found, then the BS determines that the node is replicated. Based on the fact that an uncompromised mobile node should never move at speeds in excess of the system-organized maximum speed. As an outcome, an uncompromised (original) mobile sensor node measured speed will appear to be at most the system- organized supreme speed as long as speed measurement system with low error rate is employed. On the other side, duplication nodes will appear to travel much faster than original nodes, and thus their measured speeds will possible be over the system-configured supreme speed because they need to be at two (or more) different places at last. Therefore, if it is detected that a mobile node measured speed is over the system-configured maximum speed, it is then extremely likely that at least two nodes with the same identity are present in the network. By leveraging this perception, the SPRT is achieved on all mobile nodes using a null hypothesis that the mobile node has not been repeated and an alternate hypothesis that it has been repeated. In using the SPRT, the occurrence of a speed that either reduces or beats the system-configured supreme speed will lead to acceptance of the null and alternate hypotheses, correspondingly. Once the substitute hypothesis is accepted, the replica nodes will be revoked from the network.

V. DETECTION TECHNIQUES FOR MOBILE WIRELESS

a) Type MCW

A centralized detection is scheme for mobile WSNs by exploiting the fact that a genuine node never moves beyond the maximum speed. Every node in WSNs collects the IDs and locations of its neighbors along with their communication times, 3 and every node then transmits the collected data to the BS in an authentic way. If a node moving over the maximum speed is found, then the BS determines that the node is replicated.

b) TYPE MDW

Distributed Techniques: Extremely Efficient Detection (XED): extremely efficient detection (XED), against node duplication attack in mobile sensor networks. The clue behind XED is motivated from the observation that for the networks without duplications, if a sensor node si encounters the additional sensor node sj at earlier time and si sends a random number r to sj at that time, then when si and sj meet again, si can ascertain whether this is the node sj met earlier by inviting the random number r. Based on this remark, a “remember and challenge strategy” is proposed. Once two sensor nodes, si and sj, are within the message ranges of every other, they first, correspondingly, generate random numbers rsi -sj and rsj-si of bits, and then they exchange their generated accidental numbers. They also use a counter to record the node ID, the generated accidental number, and the received accidental number in their individual memory. In case the couple of two nodes encountered before, the above procedure is also performed such that the accidental number deposited in the memory is replaced by the newly received accidental number. The sensor node si encounters another sensor node sj. If si never encounters sj before, they exchange accidental numbers. Otherwise, the sensor node si requests the sensor node sj for the random number rsi- sj exchanged at easier time. For the sensor node si, if the sensor node sj cannot answers or reply a number which does not match the number in si memory, si announces the discovery of duplication. When the replicas meet the genuine nodes, the replicas can always imaginary that they meet for the first time. However, if the genuine nodes have a record showing that they ever met at earlier time, the duplications are also detected.

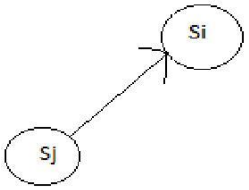

Fig.2
Generate a random number
record
and discover that the received

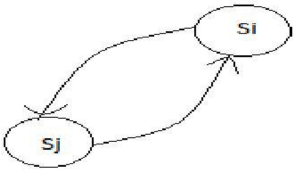

Fig.3
Check its own
number matches the
Record (Sj accept Si
as
A neighbor)

VI. CLONE DETECTION SCHEMES

Based on the above-mentioned assortment standards, we showed the simulation experiments on the representative clone detection systems with regard to discovery presentation. For this purpose, we run the simulations in each scenario for duration of 1000 s using ns-2 network simulator. All nodes uses IEEE 802.11 as a media access control protocol 6 in which the proper transmission range, and the sizes of the areas covered by static WSNs and mobile WSNs are used respectively. In order to conclude the measure of movable nodes, we employed the random trip mobility (RTM) model used. In the RTM model, each movable node travels to a accidentally chosen position with a given speed between a minimum speed (1 m/s) and a maximum speed (20 m/s), and all movable node then travels to another randomly chosen location. This random movement procedure is recurrent throughout the whole simulation period. To exam the discovery schemes under the similar simulation environments, we focused on detecting single node replications (two clones replicated from a single honest node) and then calculated the average of simulation results through more than 20 simulation experiments, which were collected and analyzed based on our performance metrics. To link the clone discovery schemes classified by the selection criteria, we measure their Ed, Pd, and Td, and then depict them, in which the x-axes describe the number of nodes in the network and the y-axes give Ed. Moreover, together values in parentheses give Pd and Td, respectively. While comparing all clone detection schemes classified by the selection criteria as shown in Fig. 2, we measure their Ed, Pd, and Td. Simulation experiments are conducted to compare their performances and then plot the graphs on the basis of comparisons, in which the x-axes describe the number of nodes in the network and the y-axes give Ed. Moreover, both values in parentheses give Pd and Td, respectively.

VII . Simulation Parameters

Table 1: - Simulation Parameters

Sr. No.	Simulation Parameters
1	Simulation time
2	Total consumed energy (Ed)a
3	Clone detection ratio (Pd)
4	Completion time (Td)b

VIII. DISCUSSION

Localized Detection: XED and EDD can battle node duplication attacks in a localized fashion. Compared to the distributed procedure, which only needs that nodes accomplish the task without the intervention of the base station, the localized procedure is a particular type of spread procedure. Each node in the localized algorithm can communicate with individual its one-hop neighbors. This distinctive is cooperative in reducing the communication overhead significantly and enhancing the resilience against node compromise. Efficiency and Effectiveness: The XED and EDD procedures can identify replicas with high detection accuracy. Notably, the storing, message, and calculation expenses of EDD are all only. Network-Wide Revocation Avoidance: The cancelation of the duplications can be achieved by every node without flooding the entire network with the revocation messages.

IX. ADVANTAGES

1. The advantages of our proposed include localized detection.
2. Efficiency and effectiveness.
3. Network-wide synchronization avoidance.
4. Network wide revocation avoidance.

X. CONCLUSION

This paper revised the state-of-the-art systems for discovery of node duplication attack also called clone attack. The present methods are generally characterized into two courses distributed and centralized. Both classes of schemes are capable in discovering and avoiding clone doses, but both schemes also have some noteworthy drawbacks. However, the present reading highlights the statistic that there are still a lot of challenges and issues in clone detection schemes that essential to be determined to become more appropriate to actual life situations and also to become accepted by the resource constrained sensor node. Model experiments are lead to relate their presentations. It is concluded that it is beneficial to utilize the grid deployment knowledge for stationary sensor networks; the scheme using the grid deployment information can save energy by up to 94.44% in similar presentation (specifically in terms of clone detection ratio and the completion time), as associated to others. On the other finger, for movable sensor networks, no existing approach works efficiently in reducing detection error rate.

REFERENCES:

[1] B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proc. IEEE Symp. Security Privacy, pp. 49–63 May 2005.

[2] 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., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[3] H. Choi, S. Zhu, and T. F. L. Porta, “SET: Detecting node clones in sensor networks,” in Proc. Security Privacy Commun. Netw. Workshops, pp. 341–350, 2007.

[4] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, “Real-time detection of clone attacks in wireless sensor networks,” in Proc. ICDCS, pp. 3–10, 2008.

[5] M. Conti, R. 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 Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Compute., pp. 80–89, 2007.

[6] Z. Li and G. Gong, “DHT-based detection of node clone in wireless sensor networks,” in Proc. 1st Int. Conf. Ad Hoc Netw., pp. 240–255, 2009.

[7] C. A. Melchor, B. Ait-Salem, P. Gaborit, and K.

Tamine, “Active detection of node replication attacks,” Int. J. Comput. Sci. Netw. Security, vol. 9, no. 2, pp. 13–21, Feb. 2009. 34 IEEE SYSTEMS JOURNAL, VOL. 7, NO. 1, MARCH 2013.

[8] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, “Random-walk based approach to detect clone attacks in wireless sensor networks,” IEEE J. Sel. Areas Commun., vol. 28, no. 5, pp. 677–691, Jun. 2010.

[9] Z. Li and G. Gong, “Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks,” in Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst., pp. 1030–1035, Oct. 2009.

[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 Trans. Mobile Comput., vol. 9, no. 7, pp.913–926, Jul. 2010.

[11] J. W. Ho, D. Liu, M. Wright, and S. K. Das, “Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks,” Ad Hoc Netw., vol. 7, no. 8, pp. 1476–1488, Nov. 2009. J. W. Ho, D. Liu, M. Wright, and S. K. Das, “Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks,” Ad Hoc Netw., vol. 7, no. 8, pp. 1476– 1488, Nov. 2009.

[12] J. W. Ho, M. Wright, and S. K. Das, “Fast detection of replica node attacks in mobile sensor networks is using sequential analysis,” in Proc. IEEE Int. Conf. Comput. Commun., pp. 773–1781, Apr. 2009.

[13] C. M. Yu, C. S. Lu, and S. Y. Kuo, “Mobile sensor network resilient against node replication attacks,” in Proc. IEEE ommun. Soc. Conf. Sensor Mesh Ad Hoc Commun. Netw., pp. 597–599, Jun. 2008.

[14] L. Zhang, Y. Hu, and Q. Wu, “Identity-based threshold broadcast encryption in the standard model,” KSII Trans. Internet Inform. Syst., vol. 4, no. 3, pp. 400–410, Jun. 2010.