Clone Detection Approaches in Wireless Sensor Networks: A Review

Ramneet Singh[1], Lal Chand[2]
Department of Computer Engineering, Punjabi University, Patiala, Punjab, India
singh.ramneet28@gmail.com, lc_panwar@yahoo.com

Abstract –
Wireless Sensor Networks are self-configured networks which consist of number of small low-cost sensor nodes that are often deployed in vigorous physical or environmental conditions for monitoring and analyzing the changes occurring in that particular environment. The concept of wireless sensor networks is used in various applications such as military surveillance, natural disaster relief, biomedical health monitoring etc. The wireless sensor nodes are very prone to a capturing attack known as clone attack. In this technique, an adversary physically captures a node from the network, spoofs its credentials, creates a replicate node and then deploys it into the network. This is possibly done to cause damage to various applications of WSNs. There are different techniques been proposed so far to detect these clone attacks in sensor networks. In this paper we will be discussing several clone detection techniques by making certain comparisons as well as proposing future related work by analyzing different parameters related to efficiency of wireless sensor networks.

Index Terms – Wireless sensor networks, clone attacks, security, clone detection techniques.

I. INTRODUCTION

Wireless sensor networks are implemented for monitoring physical and environmental conditions such as temperature, sound, motion, pressure etc. and then collectively passing the data to a base station where the data can be analysed. The base station acts like an interface between the user and the network. A wireless sensor network consists of several number of tiny, low cost sensor nodes which are deployed in very competitive environment for performing monitoring related tasks. Wireless sensor nodes use radio signals for communicating with each other. The main components of a wireless sensor node are: a microcontroller which performs tasks, processes the data and also controls the functionality of other components in the network; a transceiver which provides radio frequency based communication in the wireless sensor network; external memory for storing application or programming data as well information related to the identification of the node; a power source to provide adequate energy for communication process; sensors for measuring the physical data to be monitored. The components of a sensor node are shown in the given figure.

Due to the low cost of the wireless sensor node, it is possible to deploy thousands of sensor nodes in a particular area.

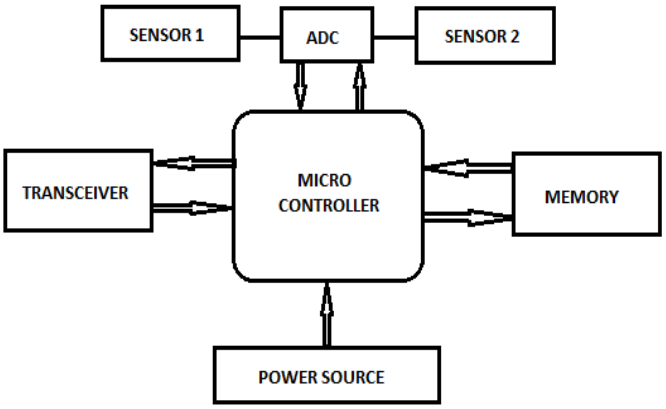

Fig.1 Components of a wireless sensor node.

These nodes require minimal amount of supervision and it is very challenging to provide efficient security functions and mechanisms for WSNs.

These sensor nodes are deployed in very aggressive environments and can be captured and compromised very easily. From a compromised node, all of its secret credentials are extracted by an adversary such as node id, nodes location, keys etc. This process is done create a replicated node against that captured node and after that large number of replicated nodes are introduced into that deployment area. Usually this is done so that an attacker can expand the compromised area

and employing clones to perform attack on the network. This phenomenon of capturing a node and extracting its information to build a replica node is known as a clone attack. The replica nodes could be authenticated as legitimate node and to launch various types of attacks like injecting false data, corrupting data aggregation, dropping data packets selectively. Thus, it is essential to detect clone nodes promptly for minimizing their damages to WSNs. Therefore, clone attackers are severely harsh and efficient and effective solutions for clone attack detection are needed to limit their harms.

In the next section, we will be discussing the centralized approach consisting of different clone detection techniques and after that distributed approach will also be explained. We will also try to analyze which technique is more efficient by their comparison using number of parameters.

II. CENTRALIZED APPROACH

In a centralized detection approach, the sensor nodes available in a wireless sensor network will send the locations and IDs of all their neighbors to a base station. The base station then verifies that each and every node should be at a distinct location. If a node with same id is detected at two different locations then there is a probability of replicated node in the network. Now, we will discuss various centralized clone detection schemes as follows:

A. Straightforward Scheme

In straightforward detection scheme given in [5], Parno et al. (2005) proposed that each node is required to send a list of its neighbors (along with their ids) and the positions claimed by these neighbors to the base station, which then examines every neighbor list to look for replicated sensor nodes. In a stationary WSN, conflicting position claims for one node id indicates a replication. Once the base station spots one or more replicas, it can revoke the replicated nodes by flooding the network with an authenticated revocation message.

This is the most basic centralized approach for detecting replicated nodes in a wireless sensor network yet it comes with several limitations. One of the drawbacks of this technique is that it causes single point of failure i.e. if any part of the system fails, it will stop the entire system from working. Also the nodes which are close to the base station will receive huge routing load which will cause rapid depletion of power supply. As we know, nodes have minimal amount of computational resources so this adds to the limitation of this technique. The nodes nearby base station are also prone to the attacks. Third some WSNs may not have the luxury of a powerful base station.

B. Area-Based Approach

The Area based clustering detection method was proposed in [9]. In this method, first of all a central node is selected which consists of maximum number of nodes within its transmission range. After that, the network area is divided into different sub-areas equally on the basis of degree of angle around the central node. Now, for each sub-area a witness node is selected. Now as it is given in the figure 2, the network is divided into three sub-areas of 120 degree each around the central node. Now, the original node A sends the location claim to its neighbor and then it further send it to the witness node W. Assume that an attacker A' or replica node also sends its location claim to the witness node which is located near the attacker. If a witness node has the location claims coming from both the original node (A) and attacker (A'), it can detect that there are conflicting location claims. Then, the witness node will broadcast the conflicting detection message to all nodes in the network. If no conflicts are found in the sub-area, the witness node will send all the location claims to the central node. On the other hand, if the witness node in each area cannot detect any conflicting location claim, they will send all collected location claims to the central node. After the central node (C) detects location claims with the same ID but from different locations, it broadcasts the conflicting detection message to all nodes in the network. This technique avoids single point failure of central node while decreasing communication overheads and maintains the network lifetime.

C. Cloned Key Detection

This technique was proposed by Brooks et al. (2007). A clone detection protocol based on random pairwise key pre-distribution schemes [1] was proposed

which is quite different from other approaches. This method is used for detection of cloned keys rather than the replicated sensor nodes. The keys given to each and every node follow a certain pattern. Therefore, It is possible to monitor the key usage (which refers to the number of times a key is used to set up a secure connections between neighboring nodes, but not to the time a key is used for encrypting or decrypting packets) as authentication tokens and then detect statistical deviations that indicate clone attacks. The approach detects the cloned keys by analysing node authentication statistics; those keys whose usage exceeds a certain threshold are considered cloned and erased from the network. To this end, each node is required to report its pre-loaded keys to the base station, which then performs an anomaly detection to discover cloned keys. This technique is effective when a high false positive rate is set and more clones exist in the network and all nodes having a key of small size.

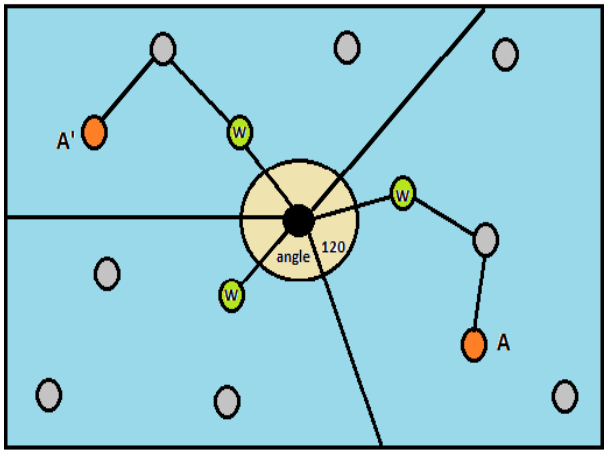

Fig.2. ABCD detection scheme where A is the original node and A' is a replicated node.

D. Set Operations

In this technique proposed by Choi et al. (2007), the operations intersection and union operations of exclusive subsets in the network are used which are computed to reduce the detection overhead [2]. In this technique, logical partitioning of network is done by SET. The network is divided into non-overlapping regions also known as clusters. These clusters are managed by their respective leaders or cluster heads. The cluster heads report to the base station all the credentials of the nodes available in its region including the leader itself. This information is in the form of subset (which is a subset of all node ids network-wide). Intuitively, the ‘‘intersection’’ of any two subsets of reports should be empty; otherwise, a replication is detected. Essentially, all node ids in the network are pulled up by the base station and left to its discretion. It is exactly noted that reporting every node's id to the base station may cause the size of the report to become too large, and this problem can be ‘‘addressed’’ by using randomized ‘‘optimization’’, where a leader (cluster head) only generates a report of randomly selected members instead of all nodes in the managed region (cluster). Taking additional security mechanisms such as message authentication codes into consideration, such multiple-round ‘‘optimization’’ inevitably results in even higher detection cost in terms of computation and communication.

III. DISTRIBUTED APPROACH

In the distributed approach of clone detection, every node collects all of its neighbor's identities along with their locations and broadcasts to the network. Though the distributed approaches cause high communication overhead, but these are considered more efficient than centralized approach. Now, we will discuss various distributed clone detection techniques.

A. Node-to-Network Broadcasting

This is a very simple and efficient approach for clone detection in wireless sensor networks. In this method [7], every node gathers all its neighbors' ids and their positions, and broadcasts it to the entire network. When a broadcast message is received by the node, it compares those nodes listed in the message with its own neighbors. Once nodes that have conflicting positions are spotted, they can be revoked also with authenticated broadcasts. The main problem of N2NB technique is that it causes a high communication overhead which reduces the efficiency of the technique up to some extent.

B. Line Selected Multicast

In the Line-Selected Multicast (LSM) [9] approach, a location claim for each sensor node is transmitted along some random line segments in the network. The location claims will be stored at sensor nodes along the line segments. The idea of LSM is that the line segments for two conflicting location claims are likely to intersect and

the node at intersection can detect the replication because the conflicting claims have the same ID but come from different locations. The process of LSM method can be illustrated in Figure 3. The location claim of node A is transmitted via its neighbors. Then, the neighboring nodes select destination nodes randomly and send the location claim of node A via intermediate nodes to each destination node. If node A is compromised and the adversary's replicating node A' also send node location claims with the same node ID, the conflicting location claims are likely to be detected at some intermediate nodes.

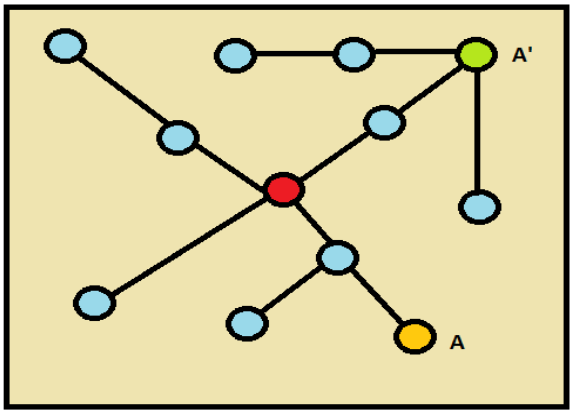

Fig.3 LSM Method in which A is the victim node and A' is a replicated node

C. Randomized Multicast

In Randomized Multicast (RM) [7] scheme each sensor announces its locations and each of its neighbors can send a copy of that claim to randomly selected nodes (i.e. witness node) and exploiting the birthday paradox effect to detect the clone nodes. Witness node can receive two different location claims with same ID and then considered the corresponding node as replica node that could be revoked from the network. The randomized multicast technique requires high storage cost while the communication for this method is similar to that of node-to-network broadcasting.

D. Random Walk Based Approach

Since Randomized Multicast has a very high communication overhead, Random Walk based technique (RAWL) was proposed. In this technique [8], each node broadcasts a signed location claim. The probability is that the neighbors of each node will forward its location claim to some randomly selected nodes. Each randomly selected node sends a message containing the claim to start a random walk in the network, and the passed nodes are selected as witness nodes and will store the claim. If any witness receives different location claims for a same node ID, it can use these claims to revoke the replicated node. 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.

E. Location and Time Based Approach

This approach is based on the grid deployment knowledge to detect the clone nodes by considering nodes location and ID. In this technique [6], first of all a deployment zone is pre-defined for the sensor nodes. Then a neighbor discovery process is followed in which every sensor node discovers the set for neighbors and asks for an authenticated location claim from every sensor node. If the distance between the two nodes is within its transmission range, that node will be trusted as a neighbor. After deploying a group of nodes, they will be preloaded with a time stamp signed by a server. This time stamp indicates that the sensor nodes in the group should finish neighbor discovery before the time given. If they try to set up connections with other nodes after given time, they are considered to be untrusted nodes. After this each and every sensor node forward its own location and ID to the neighboring nodes for clone detection process. If any node received two different location claims with the same ID, the collision occurs and the clone node will be detected. This technique consumes lesser energy as compared to other detection schemes. The LCA technique uses DSDV routing which consumes more battery power as in case of DSDV routing regular updating of table is required.

F. RWS and MRWS Protocols

These two protocols were proposed in [3] determining distributed clone detection method. In RWS (Random Witness Selection) protocol, each node consists of a private key and a public key. The node uses the private key to sign to its location claim and other

nodes verify the same. So when a node broadcasts a signed location claim to all its neighbours, each neighbour verifies the signature and checks the transmission range between the nodes. If the node is within the transmission range it initiates the counter by 1. Then the claim is sent after verification and after incrementing the counter. It will reach to its random neighbour and it verifies the signature and forwards it again until the counter reaches the maximum number of walks. Whenever a collision is detected i.e. 2 different claims with the same ID, the two conflicting claims are broadcasted as an evidence to revoke the replicas. Each node receiving the two claims independently verifies two signatures. If two signatures are valid, it terminates the link with the replicas. MRWS (Minimized Random Witness) Protocol is the modified form of RWS. It was mainly proposed to reduce the memory cost of the RWS protocol.

IV. CONCLUSION

In this paper, we discussed a major security issue of wireless sensor networks known as clone attacks and its detection. We classified some traditional and recently advanced detection protocols as centralized and distributed and reviewed the literature. We reviewed recent research work for e.g. in centralized approach; the area based clustering detection was discussed which is a better centralized solution than distributed LSM technique. Though distributed clone detection techniques cause huge communication overheads they are considered to be more efficient than centralized techniques. Among the distributed schemes, a recently proposed LCA approach was discussed which with the help of location and time uses a time interval mechanism to detect clones in a network. The RWS and MRWS protocols are also an efficient solution for clone detection which helps in reducing the memory cost. The main motive of recent research in this area is to find an optimal detection technique which helps in increasing the performance of network by reducing the costs and communication overheads. So, we hope that these techniques will provide complimentary mechanisms against clone attacks and help in enhancing the security aspect of wireless sensor networks.

REFERENCES

[1] Brooks R, Govindaraju PY, Piretti M, Vijaykrishnan N, Kandemir MT, “On the detection of clones in sensor networks using random key predistribution” IEEE 2007; 37(November): 1246-58.

[2] Choi H, Zhu S, La Porta TF, SET: Detecting node clones in sensor networks, In proceedings of the third international conferece on security and privacy in communications and networks and the workshops (Securecomm’07); 2007. P 341-50, December.

[3] D Sheela, Priyadarshini, Dr. G. Mahadevan, “Efficient approach to detect clone attacks in wireless sensor networks”, IEEE, 2011.

[4] Kwantae Cho, Minho Jo, Taekyoung Kwon, Hisao-Hwa Chen, Dong Hoon Lee, “Classification and experimental analysis for clone detection approaches in wireless sensor networks”, IEEE, Vol. 7, No. 1, March 2013.

[5] Parno B, Perrig A, Gligor V, “Dsitributed detection of node replication attacks in sensor networks.”, IEEE, p. 49-63, May 2005.

[6] R. Sivaraj, R. Thangarajan, “Location and Time based clone detection in wireless sensor networks”, IEEE, 2014.

[7] Wen Tao Zhu, Jianying Zhou, Robert H. Deng, Feng Bao, “Detecting node replication attacks in wireless sensor networks” *Elsevier*, 1022-1034, 2012.

[8] Yingpei Zeng, Jiannong Cao, “Random walk based approach to detect clone attacks in wireless sensor networks”, IEEE, Vol. 28, No. 5, June 2010.

[9] Wibhada Naruephipat, “An area-based approach for node replica detection in wireless sensor networks”, IEEE, 2012.

[10] Zhang M, Khanapure V, Chen S, Xiao X, Memory efficient protocols for detecting node replication attacks in wireless sensor networks, IEEE (ICNP’09); 2009. P. 284-93, October.

[11] Jennifer Yick, Biswanath Mukherjee, Deepak Ghosal, “Wireless Sensor Network Survey”, Elsevier, 2292-2330, 2008.