Location Traced Hybrid Detection of Node Replication Attack in Mobile Wireless Sensor Network

B.Gowtham
Student, Department of Information technology
PSG Polytechnic College, Coimbatore.

S.Sharmila
Department of Information technology,
PSG Polytechnic College, Coimbatore.

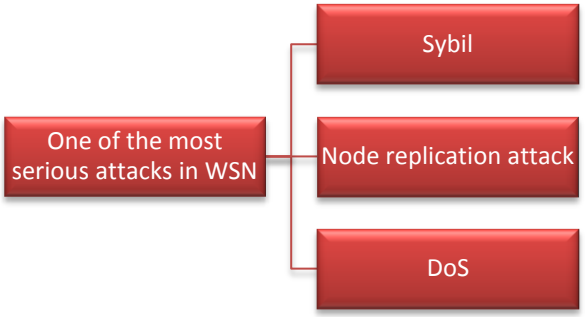
ABSTRACT

The wireless sensor network is used to solve problems in real world such as industrial and environmental Sensing. There are two types of Wireless Sensor Network, Mobile and Static. They are the Wireless Sensor Network are prone to attacks. The most prominent attack in Wireless Sensor Network is node replication attack were the nodes are replicated virtually. The replicated node captures the key or id of the node, makes copies of the node in the network with the same id and may cripple the entire network. It is even more difficult to detect them if they are in a mobile network. The scheme proposed is for a mobile Wireless Sensor Network where the location makes the detection of replication attack even more challenging. The proposed scheme will not only trace the location using array of the locations in the mobile sensor network, but also detect the replicas using multiple scenarios such as id recognition and neighbor replica detection. The scheme can efficiently detect and make way for defense in the network.

1. INTRODUCTION

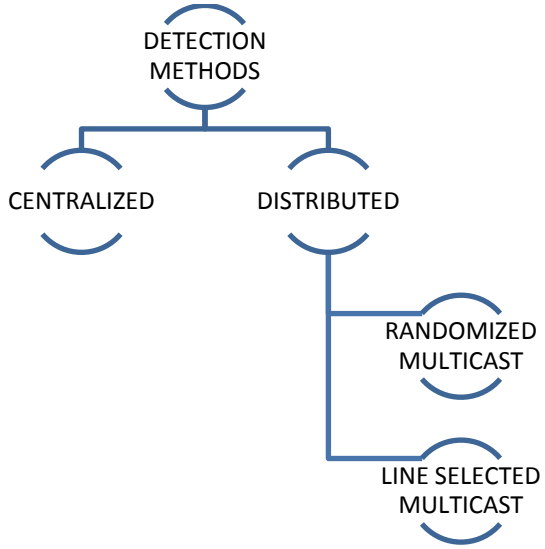
Wireless sensor networks is a network were the nodes or sensor of the network senses the environment around them.This sensed information is then sent to a base station that is locally located or to a station remotely located. In case of remote data transfers the data could be received by a local station and can be forwarded or using a satellite or other wireless transfers sending the data directly to the remote base station. Wireless sensor networks can be of two types. One is a static Wireless Sensor Network and another is a mobile Wireless Sensor Network.In a static Wireless Sensor Network the nodes in the network do not move. The mobile is a scenario were thenodes of the network moves sensing the environment. These sensor networks are used to monitor environmental changes in places were the conditions are not sustainable for prolonged existence of human, such as near the volcanic mountain's peaks, Antarctic areas were temperature may be at subzero, or used in industries for monitoring of instruments were it might be difficult for monitoring using labor such as in nuclear plants, mines or in chemical factories, in warfare were constant monitoring is difficult or impossible.

The Wireless Sensor Network also comes with disadvantages. An unprotected network could be prone to different type of attacks were the attacker tries to steal information or cripple the network. There are different types of attacks. Some of them are Denial of Service (were the attacker denies the service of the node), Sybil attack (were the attacker steals a key of the node, changes and releases many nodes with different key or id virtually crippling the system) and node replication attack (attacker steals the id or key, replicates them and launces them virtually over the network). In these the Node Replication Attack is the most prominent one. Here the attacker steals the cryptographic key used to identify the node, copies and launches the node in the network thereby creating virtual copies of the captured node, uses them to send false data or to cripple the network so that either there is no sensing network or there is no reliable information. This creates major problems especially in warfare sensor network were the monitoring is constantly required. For instance mobile sensor network monitoring a group of mobile devices such as mines setup in the field and if the hacker replicates them the real mine cannot be identified. If it is on a large scale, there will be no particular information about the mine. Thus there is a necessity in protecting the sensor network for attacks.



2. EXISTING METHODS

There are several methods proposed for detection of node replication attacks in wireless sensor networks. There are two types of detection schemes. They are centralized and distributed. Some of the proposed methods in distributed are Randomized multicasting and line selected multicasting. Both these algorithms are useful for detection of node replication attack in wireless sensor networks in a small sector or area. The centralized detection is useful for detection or node replication attack in a large scale comprising of the entire network. In both the algorithms, the nodes have a secret encrypted ID where the encrypted id is sent or transmitted. In distributed scheme the sender sends the id to the receiver through their neighbors. If the receiver finds the id correct, the next node sends the information. Ifit is not correct then a defensive mechanism is launched.



3. DISTRIBUTED DETECTION SCEMES:

LINE SELECTED MULTICASTING

In case of line selected multicasting, the receiver and the neighbor nodes which receive the id are preselected and send. Here the information is encrypted and sent via the neighbor the detection of replicas are simplified. If the neighbors receive the id correctly the information is passed. If the neighbors do not receive correctly the defensive mechanism is called. The drawback is that if there is a large scale attack on the network, the scheme is not efficient as the attack happens in many places using the same id the nodes located remotely might take the replica for a real node.

4. RANDOMIZED MULTICASTING

In the case of randomized multicasting, the sender and receiver are selected according to the probability model. The probability model will choose the neighbors for sending the id. The encrypted id is sent through the neighbor. Here detection can be simple. If the neighbor receives an id not parallel with the model or receives multiple node claims to be the same, the defensive mechanism is revoked. The drawback is that if the probability model is known to the attacker, the attacker can replicate the nodes without fear of detection. It is also hard to implement on a very large scale.

5. CENTRALIZED DETECTION

The centralized detection scheme is a detection scheme where the nodes in the network send their id to the centralized node so that it can detect the replicas in the node and launch the defense mechanism. This is efficient because it clearly identifies the replicas. But the drawbacks are that the central node if captured will lead to the destruction of the entire network. If the central node is captured, sensed information of the entire network is rendered useless as the attacker can now replicate any number of times without detection. There is also another problem. If the central node fails or is destroyed, it leads to the failure of detection of entire network henceforth the detection scheme fails.

The following table gives the information about the types of current schemes proposed for detection of node replication attack in wireless sensor network. The proposed scheme can overcome the drawbacks in the current systems.

PROPOSED SYSTEMS	DESCRIPTION	DRAWBACKS
centralized detection	Nodes communicate with a central node and send the id.	failure in central disables the network and if central node is captured the scheme fails
randomized multicasting (distributed)	the nodes are selected by probability model and send via neighbors	if the probability model is compromised the detection scheme fails
line selected multicasting (distributed)	the nodes are selected by preprocessed line selection method	Not efficient in detecting the attack over a large scale.
Sequential Probability ratio test (hybrid)	a centralized scheme were the probability is seq. considered by ratio	Uses a lot of power for processing and costs more.

6. PROPOSED SCHEME

The scheme that is proposed will be a hybrid scheme comprising both central and distributed detection schemes. The network can have a large area for sensing. The area is separated into 'sectors'. Thus it is a distributed system. Each sector has a central node were the nodes can send their id for checking. Thus it is also a central in a sector wise analysis. Then as it has both the central and the distributed detection scheme hence it is a hybrid scheme.

Fig1.1 shows the area for sensing and there are local sectors were the sensing is required. Each local sector can have array separated partitions were nodes can be present

The proposed scheme is separated into sectors. Each sector has an array separation. Each array area or 'cell' can contain one node. In the central portion of the array, a 'central node' a node that sends, receives and process the data with each node. Each sensor node has an inbuilt encrypted key or id. The central node acts like a server (computer server). It can send request and receive data. The central node can act both as a node that sensor the environment and also as a node which can detect node replication attacks or it could be a dedicated node for detection of node replication attack over the network.

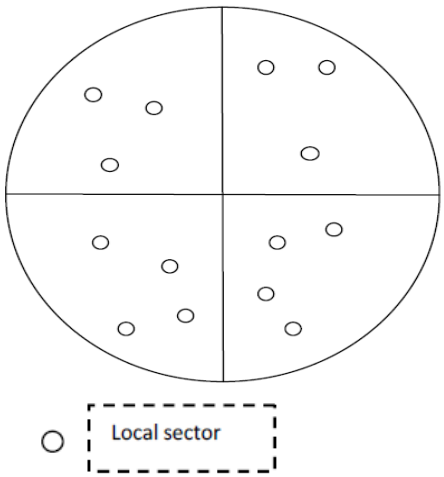


FIG 1.1 sectors over the area.

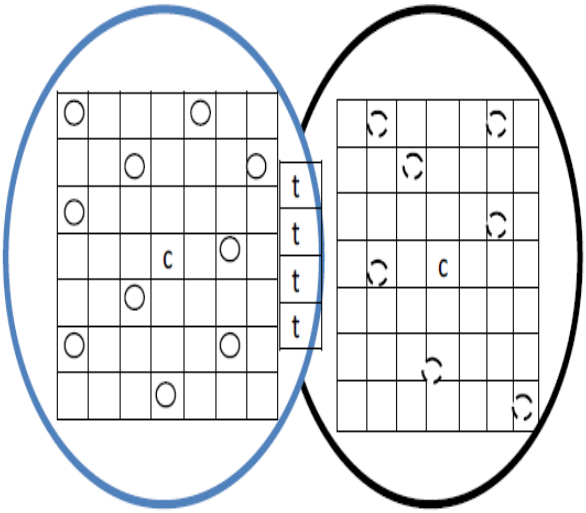


Fig1.2 two sectors overlapping in a crowded environment.

The sectors have a temporary node and using them the nodes can be moved from one sector to another.

6.1 Detection method

The detection used a hybrid form were the central and distributed schemes are combined. The local sector follows a centralized scheme and the entire network has distributed local sectors. An array tracking method is used to detect the attack. The local sectors are separated into an array and the array is used for giving the location id for the nodes. For example the array are for a node can be 2, 3 denoting the location. This is maintained by the central node. The central nodes have a table of the location of the nodes in the array.

The central node sends a request for the id of the sensor. This id is encrypted either using blowfish or using hashing functions. The requested sensor sends back its ID. The id send will contain the location of the node and its cryptic key. Then after receiving the key, if it is correct, then the central node will send the request of the nearby neighbor node identified by the table present in the memory of the central node. The neighbors will sense the node and send to the center. This will prove that the node is present in the correct location. If the neighbor check is not correct, the defensive mechanism will be revoked. In this process if the center receives more than 1 id a defensive mechanism is revoked.

In mobile networks, if the mobile has to move from place to another in the array field, the node sends a request for movement to the center. It will in the format of (present node location, next node location; key). The central node updates the location after sending the acknowledgement to the node that is to be moved. It the movement is cancelled, the node sends information to the central node.

6.2 Detection in central node attack:

There might be a possibility of replication of the central node itself. In such a scenario the central nodes will use a randomized scheme to detect if there are any replicas in them. The central systems have a separate communication frequency that is powerful enough to transmit it throughout the area of WSN. If the central nodes are replicated, a defensive mechanism is revoked.

7. CONCLUSION

Thus using three replica identification schemes in the single scheme and tracing the location of each node, the replication attack on wireless sensor network can be detected. This scheme can be effective in wireless nodes in WSN. Although the processing is complex in the system and so there might be a requirement for a central node to be dedicated for communication purpose this is better for mobile replication attack and might be cost effective.

8. REFERENCES

[1] Distributed Detection of Node Replication Attacks in Sensor Networks, Bryan Parno, Adrian Perrig, Carnegie Mellon University; Virgil Gligor, University of Maryland.

[2] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized,Efficient, and Distributed Protocol for the Detection of NodeReplication Attacks in Wireless Sensor Networks," Proc. ACM MobiHoc, pp. 80-89, Sept. 2007.

[3] D. Braginsky and D. Estrin. Rumor routing algorithm for sensor networks.In Proceedings of ACM Workshop on Wireless Sensor Networks and Applications, 2002.

[4] A. Hu and S. D. Servetto. Asymptotically optimal time synchronization in dense sensor networks.In Proceedings of ACM International Conference on Wireless Sensor Networks and Applications, 2003.

[5] P. Rohatgi. A compact and fast hybrid signature scheme for multicast packet.In Proceedings of ACM Conference on Computer and Communications Security (CCS), Nov. 1999.

[6] Choi H, Zhu S, La Porta TF. "SET: Detecting node clones in sensor networks" In: Third International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm 2007); 2007. p. 341–350

[7] Zhu B, Addada VGK, Setia S, Jajodia S, Roy S. "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks" In: Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007); 2007. p. 257–267

[8] Yuichi Sei , Shinichi Honiden , "Distributed Detection of Node Replication Attacks resilient to Many Compromised Nodes in Wireless Sensor Networks", 2008 ICST

[9] Chia-Mu Yu, Chun-Shien Lu and Sy-Yen Kuo, "Efficient distributed and detection of node replication attacks in mobile sensor networks" IEEE 2009.

[10] Xiaoming Deng, Yan Xiong, and DepinChen , "Mobility-assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks" 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications

[11] V.Manjula and Dr.C.Chellappan, "The Replication Attack in wireless Sensor Networks: Analysis & Defenses" , CCIST 2011, Communications in Computer and Information Science, Volume 132, Advances in Networks and Communications, Part II, Pages 169-178, book chapter, Springer – Verlog.

[12] M. Conti, R.D. Pietro, L.V. Mancini, and A. Mei, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," Proc. ACM MobiHoc, pp. 80-89, Sept. 2007.

[13] B. Parno, A. Perrig, and V.D. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 49-63, May 2005.

[14] Jun-Won Ho, Matthew Wright and Sajal K. Das, "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

[15] J. Ho, D. Liu, M. Wright, and S.K. Das, "Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1476-1488, Nov. 2009.