Journal of Computer Science and Applications.
ISSN 2231-1270 Volume 7, Number 1 (2015), pp. 29-38

http://www.irphouse.com

Replica Node Attack Detection Approaches in Static WSNs

Geetha C[1] and Ramakrishnan M[2]

[1]*Research Scholar, Manonmaniam Sundaranar University, Tirunelveli*

[2]*Professor and Chairperson, School of IT, Madurai Kamaraj University, Madurai*

ABSTRACT

Wireless sensor network is a collection of sensor nodes. The sensor network is infra- structureless and they are often deployed in military, healthcare, civil and weather-forecasting applications. As the applications of wireless sensor networks increases, there are many issues related with security also raises. Nowadays a common issue in this network security is intrusion detection. The sensor nodes are power constrained; resource constrained and so easily attacked by malicious nodes. One of the major attacks is node replica attack. A node captures the id and cryptographic information of another node and replicates this node and distributed in the network which will lead false data transmission, leaking the data, jamming the data transmission etc. The paper proposes two different algorithms to detect replica node attacks. One is based on a token which is generated by the source node. Other one is based on hash-secret code generated by a server. These algorithms both show high efficiency in detecting the clone nodes easily and simply. All the messages are combined into one token and so this reduces the number of message transmission also. In the second method it uses the secret hash code and so it authenticates the sensor nodes. The simulation results shows that the detection rate is high and the communication overhead is less compared with other existing algorithms.

KEYWORDS: message; replica attack; sensor network; secret hash code; token; witness node

I. INTRODUCTION

A wireless sensor network consists of spatially distributed sensor nodes. In a WSN, each sensor node is able to independently perform some processing and sensing tasks. Furthermore, sensor nodes communicate with each other in order to forward their

sensed information to a central processing unit or conduct some local coordination such as data fusion. Major applications of WSN are environmental monitoring, health monitoring, traffic control, industrial sensing, and infrastructure security. The various security attacks in WSN [1] are classified as follows:

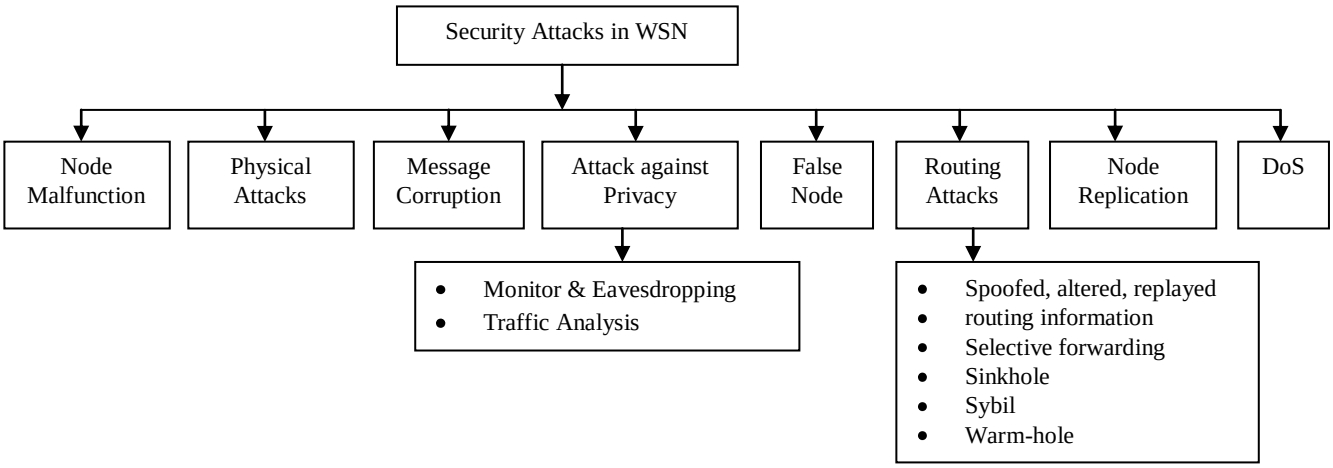

Figure 1. Security Attacks in WSN

Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.

In other words, Node replication attack is an application-independent attack unique to wireless sensor networks. The attack makes it possible for an adversary to prepare her own low-cost sensor nodes and induce the network to accept them as legitimate ones. To do so, the adversary only needs to physically capture one node, reveal its secret credentials, replicate the node in large quantity, and deploy these malicious nodes back into the network so as to subvert the network with little effort.

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.

II. RELATED WORK

The algorithms developed so far are classified in to centralized and distributed. Centralized algorithms are having the major drawback as single point of failure. All algorithms are based on id and location.

The first solution for clone detection is centralized one based on the Base Station. Each node sends the id and location information to the Base Station [2]. From the same id, if location information is received is different, clone node is detected [3]. But this scheme has drawbacks as lot of message transmission and single point of failure. Also the nodes which are located closer to BS have to transmit lot of messages and thus reduce the operational life of these nodes.

Another centralized approach is, each node is having a set of symmetric keys which are selected randomly from a large pool. Each node counts the number of times that key is [4] used for its communication [5,6]. Each node sends its count to BS. From this count, the BS identifies the clone node in network. The node which uses the keys too often are considered cloned and the revocation procedure is invoked.

Another protocol for detecting node replication attack is SET proposed in [7]. A number is generated randomly and it is sent to all nodes and it is used to form clusters and cluster heads. Within each cluster one or more trees are defined over the network graph. A protocol is used to collect all the nodes belonging to these subsets. If different subsets are having the same ID then there is a clone

The two main protocols appeared in [8] are distributed solutions. The first scheme, Randomized Multicast (RM), sends the information about its location to direct neighbours and in turn each of these neighbours sends this 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. The advantage is high detection probability using relatively limited number of witnesses. The number of messages send by each neighbour is $\sqrt{n}$.

The second scheme, Line Selected Multicast (LSM), uses the routing information 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 and saves the claims. For example, a node *a* and clone *a'* in the network. Neighbour 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 it revokes the cloned node. Otherwise store the claim and forwards to the next node. The advantage is less communication cost, high detection rate and less storage requirements.

In [9], two more schemes are proposed which are Single Deterministic Cell and Parallel Multiple Probabilistic Cells. In the first scheme, each node ID is associated with a single cell. The location information is send to the predefined witness node within a cell. Once the witness node receives the message, it is broadcasted to all other nodes in the cell. In second scheme, A number of witnesses are determined and it is already defined. The neighbours of a node *a* send *a's* claim to these witness nodes with a probability. This solution shows a high detection probability.

The X-RED algorithm selects the witnesses in a dynamic direction and broadcast the message to all its neighbours in the communication range. This method also shows a very good detection probability[10]. In the other token-based approach, a token[11] is generated and passed from the source node to all intermediate nodes on the route to the destination. Every time when the message is received by an intermediate node it verifies for the clone node by checking the id and location and append its own id and location in the token and forward it to the neighbour node.

III. PROPOSED ALGORITHM

A. *Network Model and Assumptions*

We assume that the network considered is static: the nodes are not having mobility capability. The sensor nodes deployed distributed in the observed area of 500mx500m. We assume that each node is assigned with an ID and they have the capability of calculating the location information in the form of (x,y) coordinates by using some localization algorithms. the communication link between sensor node is considered as bidirectional [12]. It follows any one available encryption decryption algorithm for message encryption and decryption [13]. ID is the sensor node identity. Loc is location of the sensor node in the form of (x,y) coordinates.

B. ***System Architecture:***

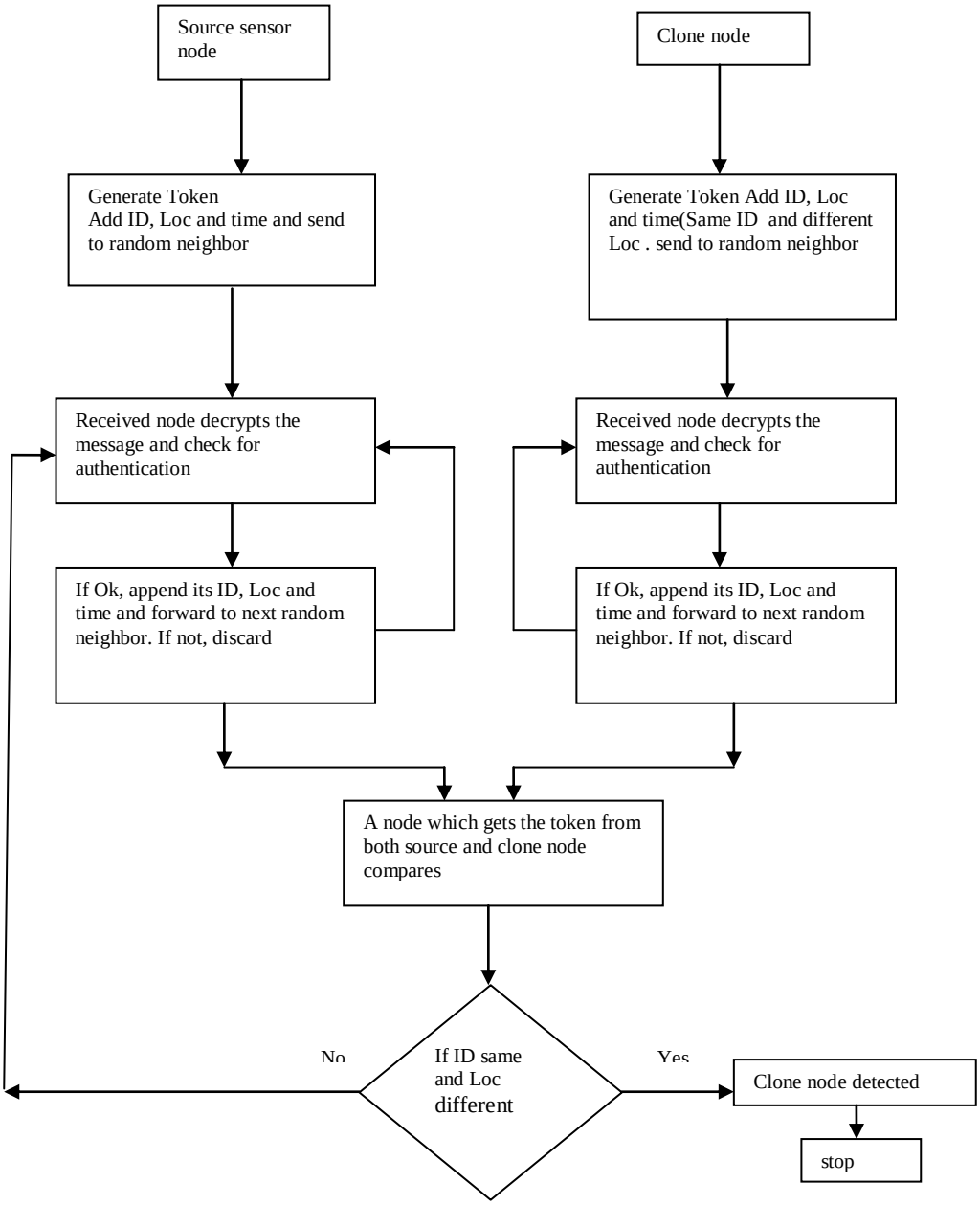

Figure 2. System Architecture for Token-Based Approach

Source node starts transmission by generating a token which contains the encrypted ID, Loc and time of the source. Randomly selects one node as the next intermediate node and forwards this encrypted message in the token. When the next node receives this token, decrypts and then verifies for authentication. If valid, append its ID, Loc and time into the token and forward to its randomly selected neighbor.

This procedure is repeated until a node called as witness node which receives the token from source and clone node. Now comparison of IDs and Loc in both the tokens are decrypted and compared. If the ID in both the taken is same and Loc is different, the clone node is detected.

C. *Proposed Model*

Token-Based Approach:

In this model, the intermediate node which forwards the token to next node is randomly selected every time. In each iteration, one node is selected as intermediate node to forward the token. In this approach the node ID and Loc are appended in to the token every time and so the token size gets increased but it is only one encrypted message. The node which receives the tokens from source node and the clone node is called as the witness node which will only performs the comparison of the contents of both tokens[11]. If clone node is detected, the revocation procedure is invoked. This approach will reduce the communication overhead.

Step 1: Source Node and Clone node generate a token.
Step 2: Add ID, Loc and Time in to the token and send to the randomly selected neighbor.
Step 3: The neighbor node after receiving the token decrypts the message and checks for the authentication.
Step 4: Checks for another token from the same ID.
Step 5: If so it is the witness node.
Step 6: Compares for same ID, cryptographic information and different Loc.
Step 7: If ok, clone node is detected. Go to Step 9.
Step 8: Otherwise append its information and forward to next randomly selected neighbor. Go to Step 3.
Step 9: End.

Secret Hash Code Based Approach:

The second method follows a secret key generated by a server. During deployment each node is assigned with a secret code generated by a central server. When a malicious node capture the cryptographic information along with this, the secret key assigned by the server is also copied. The source node transmits the packet which contains the data or payload and a secret hash code generated from the id, location and the secret key from the server. This hash code is appended by the source with the original message and transmits the message to its neighbor. When the neighbor node receives the message it is broadcasted to all its neighbors within the communication range. The clone sends the message as the original node to its neighbor. The same way hash code is generated. The hash code will be now different because the location is different, which is exactly determined by the GPS fixed in each and every sensor node. The witness node which receives multiple messages from same id will extract the secret hash code and compares. If the hash code is different it is the clone node.

Step 1: Every node will get a secret code which is assigned by the server.
Step 2: Source node computes the secret hash code from id, location and secret code.
Step 3: Append this hash code along with the original message.

Step 4: Forward this message through the shortest path to the neighbor node.
Step 5: From the clone node, the same way message is transmitted.
Step 6: The witness node, where the two messages intersect, will verify the hash codes.
Step 7: If different, there is a clone node and it is blocked from the network.

IV. SIMULATION RESULTS

These two approaches are simulated in NS2 under various densities like 25 nodes, 50 nodes, 75 nodes and 100 nodes and average is taken to plot the graphs. The figure shows the number of clones detected and the time. It shows the improvement of token based approach than the other approaches. In RED[14,15,16], the witness node is selected using pseudo-random function. It is static and the detection rate is about 84%. In X-RED[10], the witness node is selected every time dynamically and it shows the detection rate 86%. In the token based approach, it is 87% and witness node is only one, and it is selected as a node which gets the tokens from both clone and original node.

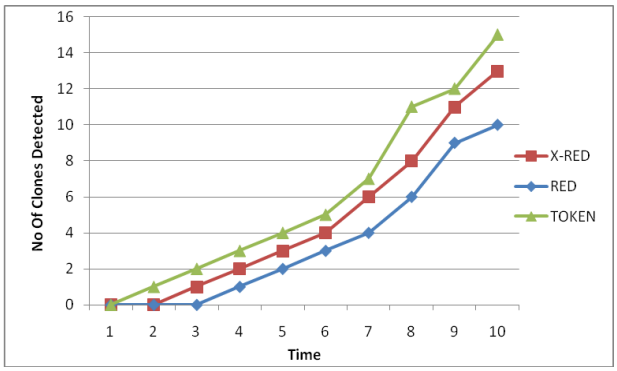

Figure 3. No of Clones Detected Vs Time (Token Based)

The figure shows Packets transmitted Vs time. Also it shows that very less number of packets transmitted during the process compared with other existing approaches. In RED, the number of messages transmitted is high and is reduced in X-RED [10] to even 0 and 1 when number of iterations goes on and it goes high during the initial stage and saturated after some time to a constant value.

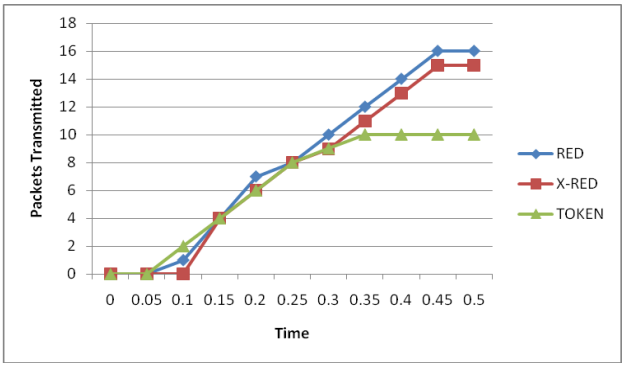

Figure 4. Packets Transmitted Vs Time (Token Based)

The following two graphs are plotted by the data taken from the outcome of the secret hash code based approach for various node density and number of iterations. The average of all above is taken and the graph is plotted. The first graph shows that the clone nodes are detected initially in slow manner because every receiver node has to compute the secret hash code and then compare. This approach will find all the clone nodes without any false positives. Sometimes the witness node itself is a malicious node; false data will be the output. In that case, the approach can't find the clone node positively. Assume that 'n' number of nodes in a network. Among these nodes some 'x' numbers of nodes are clone nodes. There are 'y' numbers of nodes selected as witness nodes in iteration. So the probability of witness node being a clone node is nC_y/yC_x.

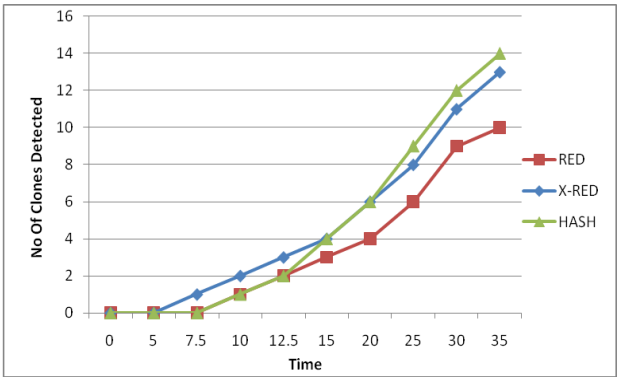

Figure 5. No of Clones Detected Vs Time (Secret Hash Code Based)

The number of packets transmitted is shown for the proposed approach and other existing algorithms. Once the clone node is detected, the packets transmitted from node is stopped and the node is removed from the network.

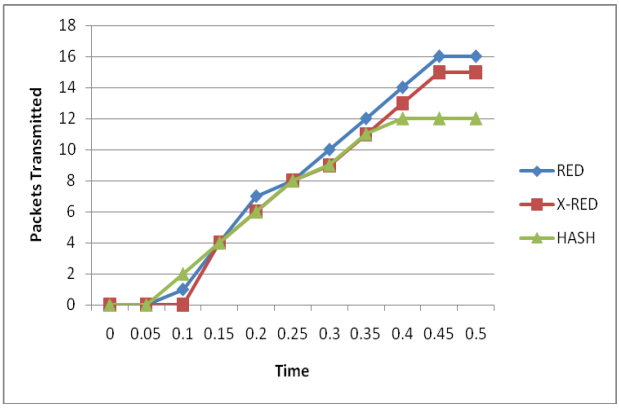

Figure 6. Packets Transmitted Vs Time (Secret Hash Code Based)

V. CONCLUSION AND FUTURE WORK

The proposed Token based approach and the secret hash code approach are the major contributions of this work. The simulation results are compared with other existing approaches and it shows that these two approaches show very good efficiency in terms of detection rate and communication overhead. The main advantage of the first algorithm is that the token is initially generated only once and every time appended the additional data. In the second approach, secret key is used to find the hash code along with location. Since the location is different the hash code generated will be different for each and every node irrespective of clone node or original node. In future, this approach can be modified for mobile sensor network

.

REFERENCES.

1. TEODOR-GRIGORE LUPU , Vasile Parvan 2,300223, Timisoara,(2009) ” Main Types of Attacks in Wireless Sensor Networks ” Recent Advances in Signals and Systems. pp. 180-185.
2. Kai Xing, Fang Liu Xiuzhen Cheng, David H. C .Du, (2008) ”Real-time Detection of Clone Attacks in Wireless Sensor Networks” The 28th International Conference on Distributed Computing Systems.
3. Wen TaoZhu, JianyingZhou, RobertH. Deng, FengBao ,(2012) “Detecting node replication attacks in wireless sensor networks: A survey”, Journal of Network and Computer Applications 35,1022–1034.
4. L. Eschenauer and V.D. Gligor, (2002) “A Key-Management Scheme for Distributed Sensor Networks,” Proc. Conf. Computer and Comm.
5. R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, (2007) “On the Detection of Clones in Sensor Networks Using Random Key Predistribution,” IEEE Trans. Systems, Man and Cybernetics, Part C: Applications and Rev., vol. 37, no. 6, pp. 1246-1258, Nov.

6. H. Chan, A. Perrig, and D. Song, (2003) "Random Key Predistribution Schemes for Sensor Networks," Proc. Symp. Security and Privacy (S&P '03), pp. 197-213.
7. H. Choi, S. Zhu, and T.F. La Porta, (2007) "SET: Detecting Node Clones in Sensor Networks," Proc. Int'l Conf. Security and Privacy in Comm. Networks and the Workshops (SecureComm '07), pp. 341-350
8. Bryan Parno, Adrian Perrig, Virgil Gligor ,(2005) "Distributed Detection of Node Replication Attacks in Sensor Networks". Published in: · Proceeding SP '05 Proceedings of the 2005 IEEE Symposium on Security and Privacy Pages 49 - 63 IEEE Computer Society Washington, DC, USA.
9. B. Zhu, V.G.K. Addada, S. Setia, S. Jajodia, and S. Roy, (2007) "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. Ann. Computer Security Applications Conf. (ACSAC '07), pp. 257-266.
10. Geetha C, Ramakrishnan M, "Xtended Randomized Efficient Distributed Detection of Clone Attacks in Static WSNs", 2014 (Online) Journal of Computer Science, pg 1900-1907.
11. Geetha C, Ramakrishnan M, "A Token Based Approach for Detecting Replica Node Attack in Static WSNs", IJIRCCE, Vol. 2, Issue 11, November 2014, pg 6501-6505.
12. Bettstetter, (2002) "On the Minimum Node Degree and Connectivity of a Wireless Multihop Network," Proc. MobiHoc '02, pp. 80-91.
13. The Original RSA Patent as filed with the U.S. Patent Office by Rivest; Ronald L. (Belmont, MA), Shamir; Adi (Cambridge, MA), Adleman; Leonard M. (Arlington, MA), December 14, 1977, U.S. Patent 4,405,829.
14. C M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, (2007) "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," Proc. MobiHoc '07, pp. 80-89.
15. M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, "Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN, (2006) " Proc. IEEE Int'l Conf. Systems, Man and Cybernetics (SMC '06), pp. 1468-1473.
16. M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, (2007) "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," Proc. MobiHoc '07, pp. 80-89.