A Token Based Approach for Detecting Replica Node Attack in Static WSNs

Geetha C[1], Ramakrishnan M[2]

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

Director, School of IT, Madurai Kamaraj University, India[2]

ABSTRACT: Wireless sensor network is a network of sensor nodes. Nowadays a common issue in this network is security. 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 proposed algorithm is based on a token which is generated by the source node. This algorithm shows 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. 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; 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 [12] are classified as follows:
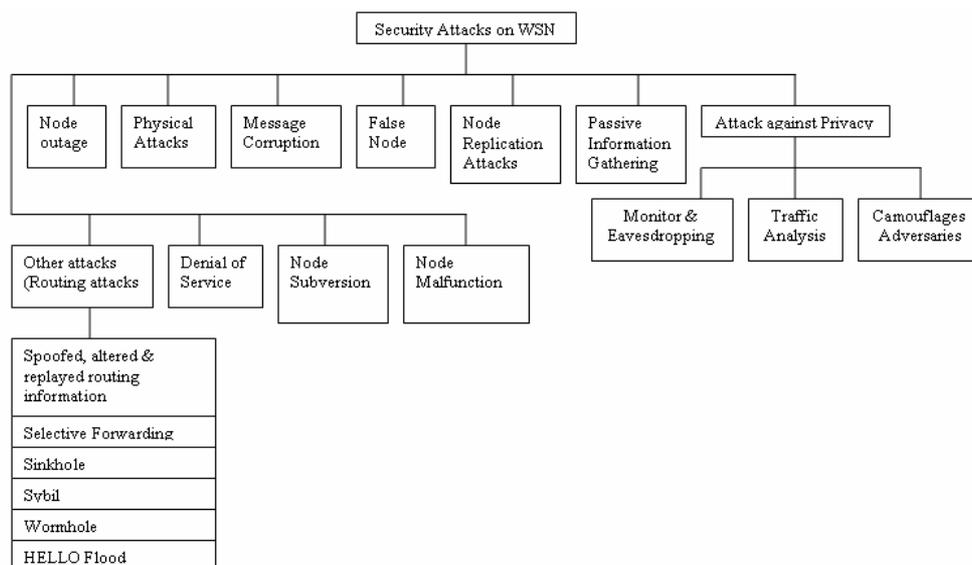

Fig. 1. Various Types of Attacks

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 [7]. From the same id, if location information is received is different, clone node is detected [14]. 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 [8] used for its communication [11,5]. 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 [6]. 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 [2] 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 [3], 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.

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 [1]. 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.
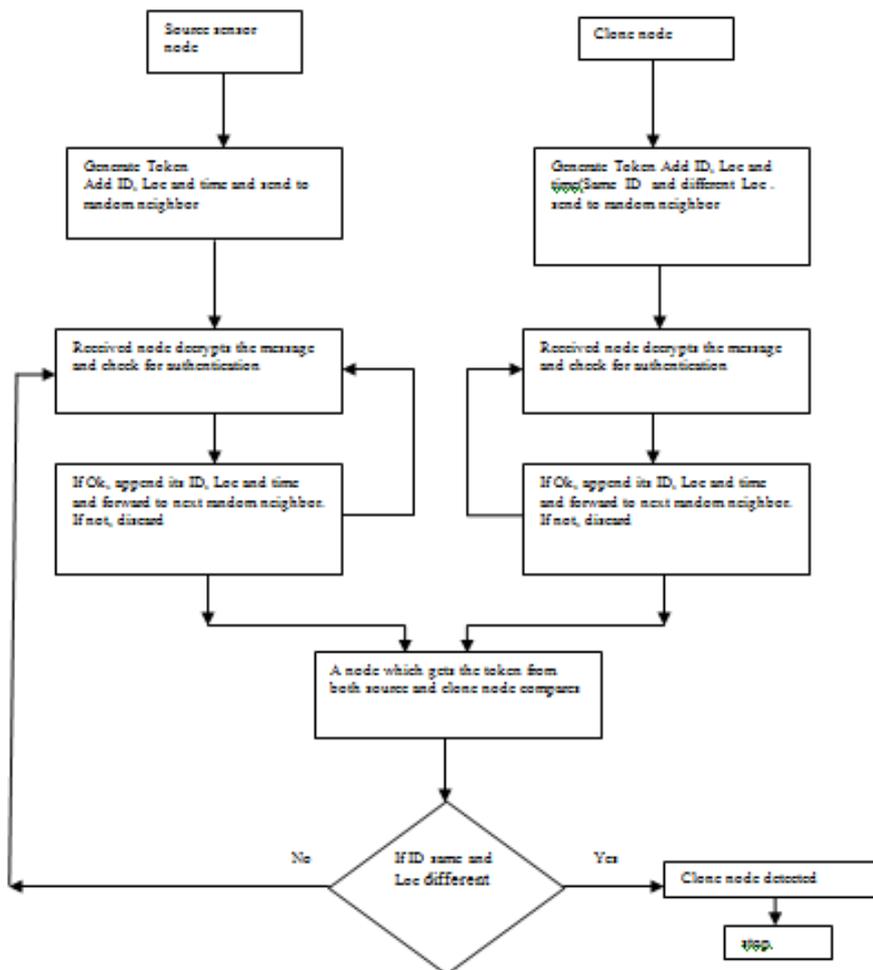
B. *System Architecture:*

Fig. 2. System Architecture

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*

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. 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.

IV. SIMULATION RESULTS

The approach is 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 Fig.3. shows the number of clones detected and the time. It shows the improvement of token based approach than the other approaches. In RED[4,9,10], the witness node is selected using pseudo-random function. It is static and the detection rate is about 84%. In X-RED[15], 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.
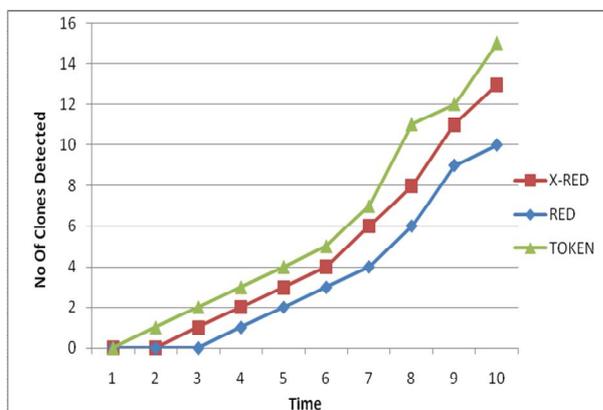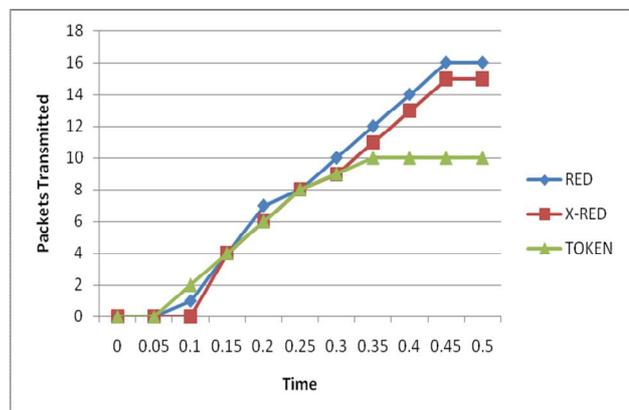

Fig. 3. Detection Rate   Fig. 4. Communication Overhead

The Fig. 4. 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 [15] 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.

V. CONCLUSION AND FUTURE WORK

The proposed Token based approach is the major contribution of this work. The simulation results are compared with other existing approaches and it shows that token based approach shows a good efficiency in terms of detection rate and communication overhead. The main advantage of this algorithm is the token initially generated. This algorithm frequently executed by all the nodes. In future, this approach can be modified for mobile sensor network also.

REFERENCES

1. Bettstetter, "On the Minimum Node Degree and Connectivity of a Wireless Multihop Network," Proc. MobiHoc '02, pp. 80-91, 2002
2. Bryan Parno, Adrian Perrig, Virgil Gligor, "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., 2005
3. B. Zhu, V.G.K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. Ann. Computer Security Applications Conf. (ACSAC '07), pp. 257-266, 2007
4. C M. Conti, R. Di 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. MobiHoc '07, pp. 80-89, 2007
5. H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. Symp. Security and Privacy (S&P '03), pp. 197-213, 2003
6. H. Choi, S. Zhu, and T.F. La Porta, "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, 2007
7. 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, 2008
8. L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. Conf. Computer and Comm., 2002
9. M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, "Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN, " Proc. IEEE Int'l Conf. Systems, Man and Cybernetics (SMC '06), pp. 1468-1473, 2006
10. M. Conti, R. Di 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. MobiHoc '07, pp. 80-89, 2007
11. R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "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, 2007
12. TEODOR-GRIGORE LUPU , Vasile Parvan 2,300223, Timisoara, " Main Types of Attacks in Wireless Sensor Networks " Recent Advances in Signals and Systems. pp. 180-185, 2009
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. Wen TaoZhu, JianyingZhou, RobertH. Deng, FengBao , "Detecting node replication attacks in wireless sensor networks: A survey", Journal of Network and Computer Applications 35,1022–1034, 2012
15. Geetha C, Ramakrishnan M, "Xtended Randomized Efficient Distributed Detection of Clone Attacks in Static WSNs", (Online) Journal of Computer Science, 2014

BIOGRAPHY

C. Geetha is a Research Scholar in Manonmaniam Sundaranar University. She received Master of Engineering in Computer Science and Engineering in 2006 from Sathyabama University, Chennai, India. Her research interests are Wireless Sensor Networks.

M. Ramakrishnan is a Director in School of IT in Madurai Kamaraj University. He received his Doctorate degree two times. He is having experience of more than 25 years and his area of interest is Network Security. He published many papers in international journals and national journals.