International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 22467-22476
© Research India Publications
http://www.ripublication.com

A Hybrid Scheme For Detecting Clone And Sybil Attacks In Wireless Sensor Networks

C. Geetha[1], M. Ramakrishnan[2]
[1]Research Scholar, M. S. University, Tirunelveli, Tamilnadu, India
[2]Professor&Chairperson, School of IT, M.K. University, Madurai, Tamilnadu, India
Email: cga.cse@rmkec.ac.in

Abstract

As the uses of wireless sensor networks in military, civil, health and other areas grows. So the security in these networks is a major concern and has to be concentrated. Since the sensor nodes are resource constrained they are easily captured by other malicious nodes in various form. Out of the various attacks, clone attack and Sybil attacks are two most common attacks. Several algorithms were developed to detect clone and Sybil nodes in wireless sensor network separately. We propose a new hybrid approach which detects both clone and Sybil nodes simultaneously. The proposed system detects clone and Sybil nodes with high detection rate. There are no false positives and false negatives. The processing load is distributed to all nodes evenly except Region Agents (RAs). In Region Agents communication and storage overhead are little high. Even then this approach uses location, id, symmetric key and also the distance between the node and RA as the information to check both the clone and Sybil nodes and detects both attacks at the same time. Since at a time multiple parameters are checked, there is no possibility to misidentify any trust node as malicious node and malicious node as trust node. The simulation results show that the proposed algorithm is efficient in terms of detection rate and provides high security.

Keywords: Clone Attack, Detection Rate, Region Agent, Sensor Network, Storage Overhead, Sybil Attack

Introduction

Wireless sensor network consists of spatially distributed autonomous sensors to monitor physical and environmental conditions such as temperature, sound, pressure and pass their data to a main location. Each sensor node has several parts: a radio transceiver, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source usually battery.

Security is a major issue in WSN as nowadays it is evolved everywhere and because of minimal resources. The different types of attacks are classified based on different criteria: passive or active, internal or external and different layers. Active attacks disturb the functionality of the network where passive attacks obtain the data transmitted thru the network without interrupting the communication(1).

Sybil and clone attacks are active attacks. A single node presents multiple identities to other nodes in the network is called as Sybil attack and an attacker seeks to add a node to an existing sensor network by copying the node ID and other cryptographic information of one node is called as clone attack(2).

A Sybil attack can misroute the data by giving false node locations(3) and paths, disturb the accuracy, divert the traffic etc.

The different types of Sybil attacks(4) are as follows:

Direct and indirect, legitimate nodes communicate directly with Sybil nodes or through malicious nodes(5). Fabricated and Stolen Identities, creates several new ids of same length or stole the ids of other nodes. Simultaneous and non-simultaneous, uses all ids at the same time or use different ids at different times.

Redundancy mechanisms are id-based. They assume that each physical node is distinguished as one entity and presents only one single abstract concept of an identity(6). Sybil attack allows ids to be forged or falsified.

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. Since the sensor nodes are resource constrained the communication overhead is to be distributed (7) evenly among all nodes.

The remaining part of the paper is organized as follows. Section 2 explains the literature survey, section 3 deals with network model and assumptions, section 4 describes the proposed methodology, section 5 discusses the results and performance analysis and section 6 concludes the paper.

Related Work

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

All sensor nodes send the id and location to the BS. When BS receives this information, from same sensor node may be different location claim received and so revocation procedure is invoked. It is single point failure and is a drawback The nodes near to the BS have to forward the messages from all the other sensor nodes to BS(8). So this is another drawback. From a large pool of keys, randomly a set of keys are selected and is assigned to each sensor node. These keys are symmetric keys(9). These keys are used by the sensor nodes during their communication. Each node counts the number of times the key is used. This count is often sent to BS. The node whose count is very high is identified as clone node(10).

Each node sends the (x,y) coordinates to its direct neighbors and in turn to its neighbors. The nodes which are receiving messages from different nodes are called witnesses and they will perform the comparison(11). If different location information is received, the replica node is present in the network. This algorithm shows high detection probability with less number of witnesses. Line Selected Multicast (LSM), uses routing information `in detecting the clone node. In addition to witness node, the intermediate nodes in the path can check for clones(11). Every time some selected number of nodes were considered as witnesses and having the capability of storing and forwarding the information. This algorithm is having less communication cost, less storage and high detection rate.

The network is divided into cells. Each cell is having number of sensor nodes associated with it. A witness node is selected in each cell(12). The location information is send to witness node and is broadcasted to all other nodes in the network by witness node. SET protocol divides the whole network in to sets and if two sets are having same ID clone node is identified(13).

The RED protocol uses a pseudo random function to select the witness node (g>=1) and then to these witnesses the location claim is transmitted. These witness nodes are having the capability to store and forward the claim messages (14). If from original and duplicate sensor nodes the claim is received by a witness node, it will perform the comparison and the revocation procedure is started.

The X-RED protocol goes in one randomly selected direction, selects one node around the circular area by computing a diameter randomly as witness node, and compares the available IDs and location with the source information(15). If matches then clone node is available. If not, the witness node forwards the information to other witness node which is selected as per the said procedure.

The existing algorithms for detecting Sybil attack are as follows:

Distribute the public and private key to all the nodes. In symmetric, each node has a unique key(16). When two nodes want to send information to each other, they send the verification message to sink node using symmetric keys and then distribute the shared key so that they can communicate.

In RRT, assume that each node can transfer via one channel at a time. To check the Sybil node, assign each node a unique channel and asks them to send an ack at a particular time. If no ack is received from a particular node, that is the Sybil node (4).

In random key pre-distribution, each node selects some k number of keys from a large pool. ID of each node is associated with set of keys of that node. By verifying the keys we can identify the Sybil node(4).

In Merkle hash tree approach, each node authenticates the IDs of all the other nodes. The Finger print approach verifies the finger prints of all neighbor nodes. Malicious nodes can't have valid finger print(8). By checking the Received Signal Strength Indicator (RSSI), identify the Sybil node(18). Having the assumption that probability of two nodes having the same set of neighbors is very low. The Sybil node has same set of neighbors for all its faked IDs(19).

A swarm agent collects the information about the routes(20). Sybil node is detected by energy variation. Clock skew is verified for all sensor nodes. Sybil node has same clock skew for all its falsified IDs(21).

Network Model

Assumptions and Model:

There are many sensor nodes randomly distributed in the network. Each node is equipped equally with same storage size, battery life, radio, computational power etc. All the nodes are static. Few numbers of nodes are malicious nodes. Each node is aware of their locations using either GPS or other localization schemes. All the nodes can communicate with one another using wireless radio channel and transmit the data using omni-directional mode. Messages transmitted by the nodes are by all nodes within the communication range. Each node is having unique ID and a symmetric key assigned by powerful server.

Performance Metrics

Detection Rate: time taken to detect the clone and Sybil attacker.

Storage Overhead: Amount of extra space required for storing the messages Communication Overhead: Extra messages transmitted and increase in size of these messages.

Proposed Methodology

Compute randomly a value using random number. Let it be diameter, D. Divide the network into circular regions using the diameter D. In each region one node is designated as Region Agent (RA). RA sends the Hello message by specifying the (ID, Loc, public key) to all its neighbors (nodes within the communication region). This step is performed in all other regions. Each and every node is asked to register their IDs with their corresponding RAs. Every node encrypts the message by using the received public key and sends the message (ID, Loc, private key, distance and start time) to RA. Private Key is used to check the authentication and start time is used to check the freshness of the message. When the RA receives these messages, it decrypts the messages and compares all the messages with one another. If the ID is different and Loc is same and the distance between the sender node and the RA node is same in multiple messages then the node is Sybil node. Again it verifies these messages for same ID with different Loc. If so, the node is clone node. Both nodes are blocked from data transmission. This is performed inside the region only. Now RAs will forward the information to all the other RAs and the above two steps will be performed. If RA fails, immediately the node among the region, having high power energy will be considered as RA and this registration process is performed in a frequent interval.

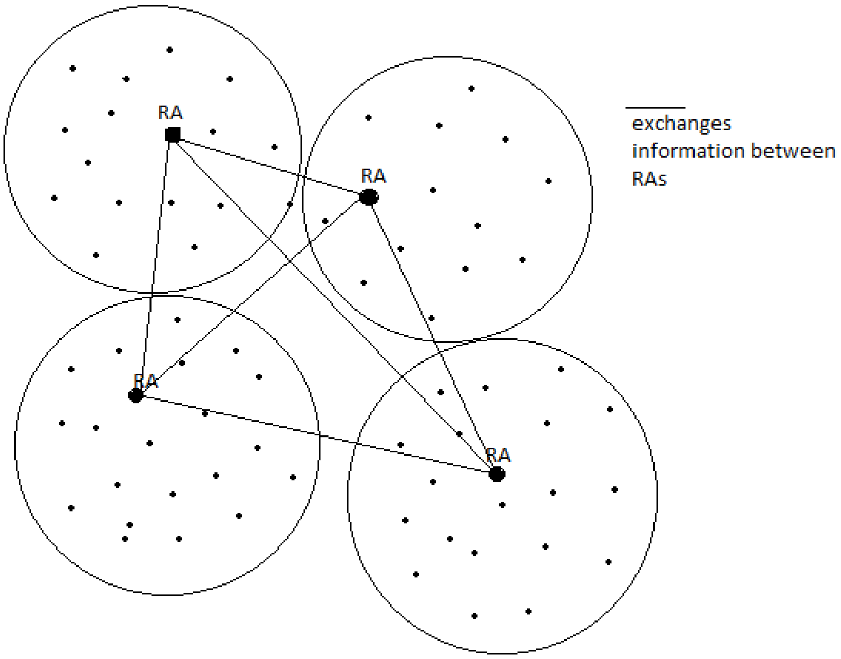

Figure 1

System Architecture

A Region Agent starts sending the Hello message to all the nodes inside the circular region which is pre-computed using random values. The nodes which receive this message will now send an encrypted message that contains id, location, cryptographic key and time stamp to RA of that particular region. The time stamp is used to verify the freshness of the message. The message is stored and decrypted by the RA. It verifies the freshness and then id, location, key and distance travelled by this packet from the source node to this RA. If multiple messages with different id but same location and distance found then it revokes the procedure to block this fake node from the network. At the same it verifies for different location and same id. If so, it detects the malicious node of type clone. Then it invokes the procedure to block the node from further communication. The same procedure is performed in all the regions. Here each RA stores n number of messages. Now all these messages are exchanged with other RAs. Let in the assumed network, there are m numbers of circular regions and each region approximately n sensor nodes are deployed. There is m RAs. After exchanging messages, each RA stores (m-1)*n messages. Fig. 1 shows how RAs are located in circular regions and messages exchanged between RAs. Fig. 2 shows the architecture diagram for the proposed method. Procedural flow is shown.

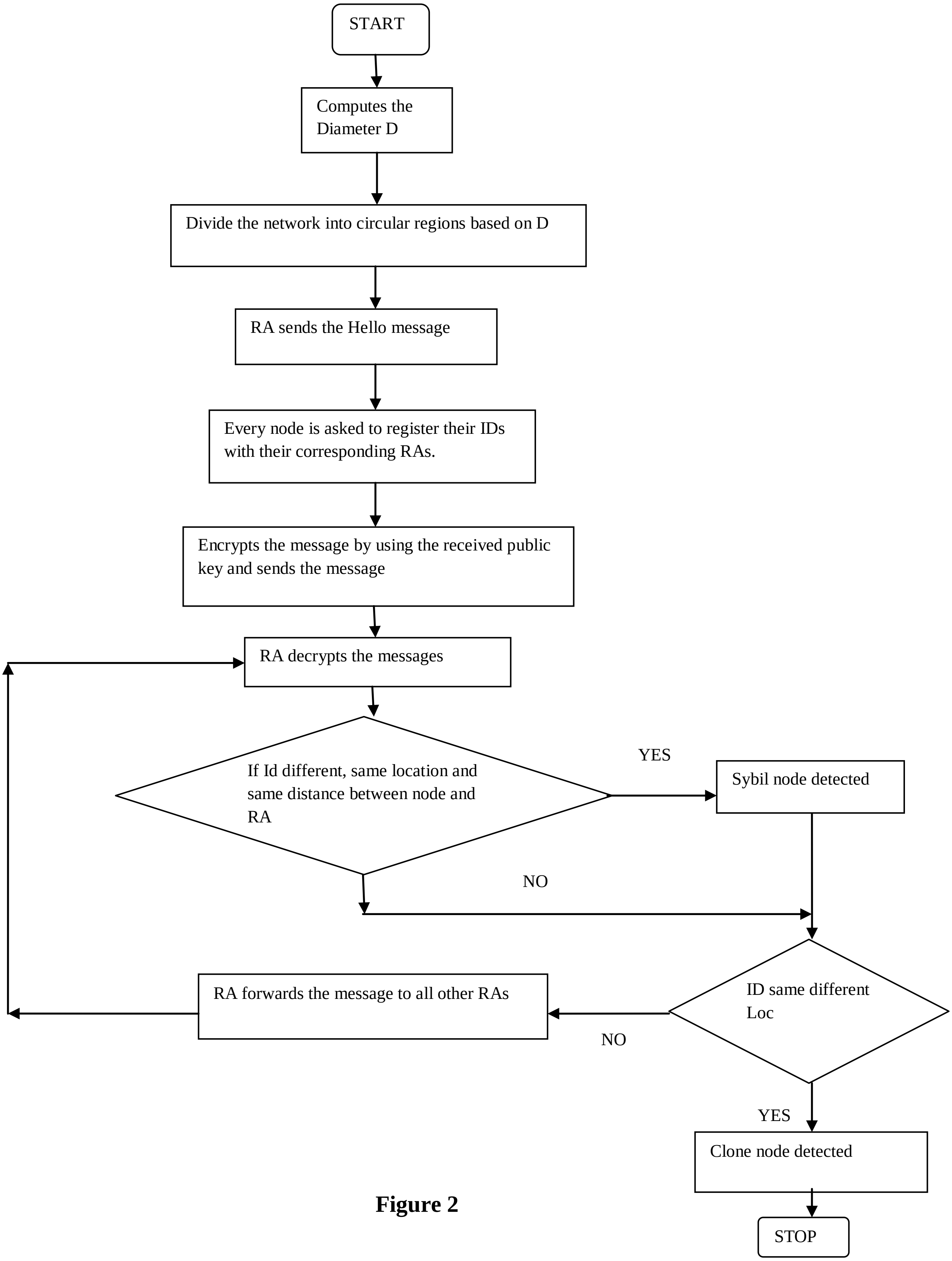
START
Computes the Diameter D
Divide the network into circular regions based on D
RA sends the Hello message
Every node is asked to register their IDs with their corresponding RAs.
Encrypts the message by using the received public key and sends the message
RA decrypts the messages
If Id different, same location and same distance between node and RA
YES
Sybil node detected
NO
ID same different Loc
NO
RA forwards the message to all other RAs
YES
Clone node detected
STOP

Figure 2

Results and Discussions

The proposed system is implemented using network simulator ns-2.35. At the time of deployment some of the malicious nodes are deployed along with trust nodes. The simulation is performed for about 500 seconds with different node density 50 nodes, 100 nodes, 200 nodes and 500 nodes.

The graph in Fig. 3 shows the detection rate of clone nodes and it is compared with RED and X-RED algorithms. The graph in Fig. 4 shows the detection rate of sybil nodes and it is compared with the existing algorithm. In existing system the graph is drawn for various densities. When the density increases the detection rate comes down(2). These two graphs show high detection rate for clone nodes and sybil nodes than existing algorithms. The data is collected under various densities and for nearly about 50 iterations and then taken the average for plotting the graphs.

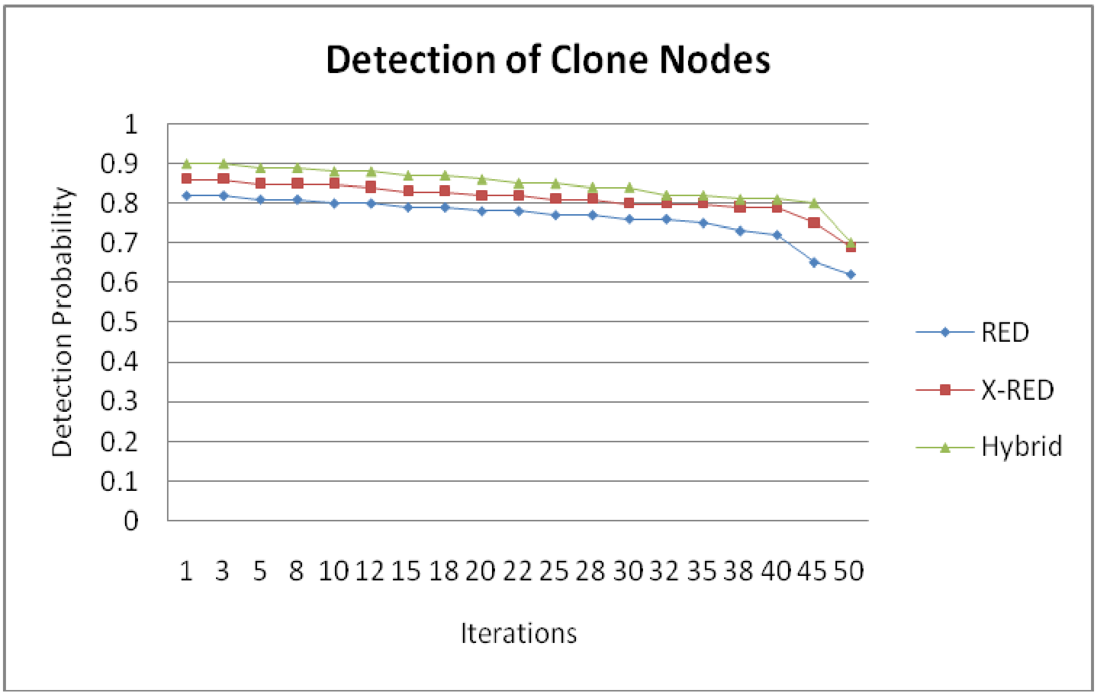

Figure 3

As per time-space tradeoff, when the detection rate is high, the communication overhead and storage overhead are naturally high. Each node in the network sent a HELLO message and received a registration message. Let the message size is p bytes.

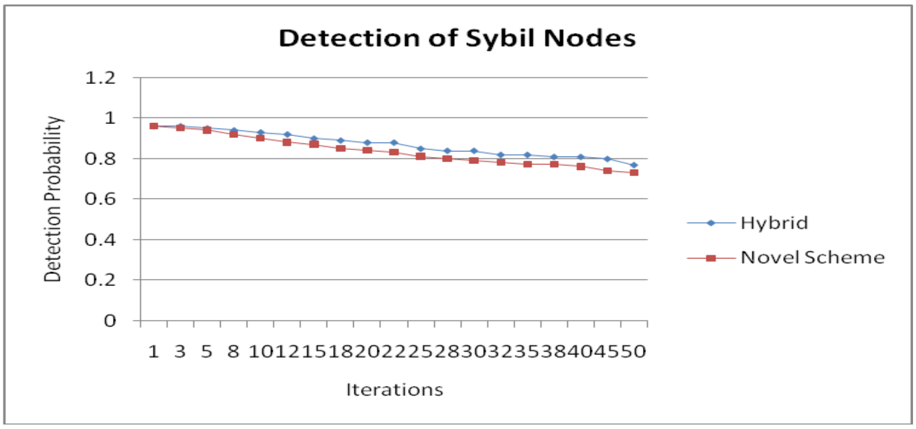

Figure 4

Region Agent(RA) compares the information with n number of received messages from n nodes in the communication range. So there are n comparisons. The message size received by each RA is np bytes. RA sends n messages to all n nodes in its communication range.

When RA exchanges the information between RAs, it sends and receives n messages of size p bytes. So totally n*n*p bytes are transmitted. The communication overhead and storage overhead are shown in the graph in Fig. 5. Both communication and storage overhead are linearly increasing with time. In X-Axis it shows time and Y-Axis number of messages. When time moves the number of messages transmitted and stored in RAs gets increased because of exchanges of messages between RAs.

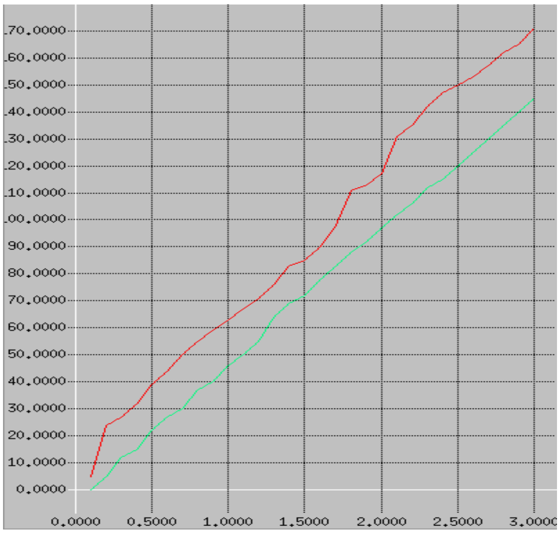

Figure 5

Conclusion

The clone attack captures a node's ID and other cryptographic information, create duplicates with these information and deploy them in various locations. The Sybil attack creates multiple fake identities and so acts as multiple nodes but in the same location. With the information like ID, location, keys, time of transmission and distance between the nodes the hybrid approach detects the clone and Sybil nodes in the network. This method does not need any hardware support. The simulation result was shown for number of nodes 500, and for 50 iterations the detection of clone attack is 90% and Sybil attack is 96%. There are no false positives and false negatives in this proposal. Based on the performance analysis, the graphs shown high detection rate.

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] G. Padmavathi and Shunmugapriya, (2009) "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2..

[3] Anuja Motarwar and Amresh Kumar, (2013) "Study on Detection of Sybil Attack in Wireless Sensor Network" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 12, pg 1184-1187.

[4] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, (2004)"The Sybil Attack in Sensor Networks: Analysis & Defenses", Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium, pp. 259 – 268.

[5] Vamsi, P. Raghu, Kant, Krishna, (2014)"Sybil attack detection using Sequential Hypothesis Testing in Wireless Sensor Networks", Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference on 12-13.

[6] Qinghua Zhang, Raleigh, Wang, P.; Reeves, D.S.; Peng Ning,(2005) "Defending against Sybil attacks in sensor networks", Distributed Computing Systems Workshops. 25th IEEE International Conference, pp 185-191.

[7] M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei,(2006) "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.

[8] K. Xing, F. Liu, X. Cheng, D.H. Du,(2008) Real-time detection of clone attacks in wireless sensor networks, in: Proceedings of the International Conference on Distributed Computing Systems, pp. 3–10.

[9] L. Eschenauer and V.D. Gligor, (2002) "A Key-Management Scheme for Distributed Sensor Networks," Proc. Conf. Computer and Comm.

[10] 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.

[11] 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.

[12] 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.

[13] 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

[14] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, (2011),“Distributed Detection of Clone Attacks in Wireless Sensor Networks” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 5, pp 685-698.

[15] C. Geetha, M. Ramakrishnan,(2014)” Extended-Randomized, Efficient, Distributed: A Dynamic Detection of Clone Attacks in Static Wireless Sensor Networks”, JCS Vol 10, Issue 10, pp 1900-1907

[16] C. Karlof, D. Wagner,(2003) “Secure routing in wireless sensor networks: attacks and countermeasures”, in: Proceedings of the IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113–127.

[17] M. Demirbas, Y. Song, (2006),”An RSSI-based scheme for Sybil attack detection in wireless sensor networks”, in: Proceedings of International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 564–570.

[18] Kuo-Feng Ssu, Wei-Tong Wang, Wen-Chung Chang,(2009) “Detecting Sybil attacks in Wireless Sensor Networks using neighboring information”, Computer Networks, Volume 53, Issue 18, 24, Pages 3042-3056.

[19] R. Muraleedharan, X. Ye, L.A. Osadciw, (2008),” Prediction of Sybil attack on WSN using Bayesian network and Swarm intelligence”, in: Proceedings of Wireless Sensing and Processing, March 2008.

[20] D.-J. Huang, W.-C. Teng, C.-Y. Wang, H.-Y. Huang, J.M. Hellerstein,(2008),” Clock skew based node identification in wireless sensor networks”, in: Proceedings of the IEEE Global Telecommunications Conference, pp. 1–5.

[21] Bin Tian, Yizhan Yao ; Lei Shi ; Shuai Shao,(2013), “A novel sybil attack detection scheme for wireless sensor network”, Broadband Network & Multimedia Technology (IC-BNMT), 2013 5th IEEE International Conference on 17-19.