Asian Journal of Information Technology 13 (7): 389-394, 2014
ISSN: 1682-3915

X-RED: A Dynamic Detection of Clone Attacks in Static Wireless Sensor Networks

[1]C. Geetha and [2]M. Ramakrishnan
[1]Department of Computer Science and Engineering,
RMK Engineering College, Chennai, TN, India
[2]Department of Information Technology,
Velammmal Engineering College, Chennai, TN, India

Abstract: A wireless sensor network is a collection of nodes organized in to a cooperative network. Each node consists of processing capability, multiple types of memory, a power source and actuators and sensors. This wireless sensor network is established in hostile and harsh environments like civil and military applications. This network is prone to various attacks. One of them is clone attack. An adversary can capture the node and replicate the node including its cryptographic information and deploy these nodes in the network. This will lead to several problems. This study proposes X-RED which detects clone nodes in the static wireless sensor networks in dynamically fast manner. It is a distributed protocol which computes the witness nodes dynamically. Researchers show that this protocol satisfies the major requirements of the distributed algorithms. Simulation results show that the protocol is more efficient than other exiting protocols in terms of detection probability.

Key words: Attacks, authentication, clone node, detection probability, direction, hash function, incoherent location, malicious node, storage overhead, wireless sensor network

INTRODUCTION

Wireless sensor network is a network of sensor nodes which are tiny with limited resources that communicate with each other to achieve a goal through the wireless channels. This network is mainly used in military applications for monitoring security and in civil applications (Akyildiz *et al*., 2002). This network is deployed in harsh and hostile environments. Based on the operating nature, it is unattended and prone to various attacks.

One of the common attacks is clone attack or replication attack where an adversary node captures some nodes and makes duplicates of the original node and thus inserts these duplicates in the network. These duplicates use the same node identifier (ID) as the original node in the network. Thus, it takes full control over the network (Lupu, 2009). The consequence of this attack is injecting false data, modifying the data, initiating a warm-whole attack and dropping packets. Thus, all these result in leaking of authorized data to an adversary. Several algorithms were developed so far to detect clone attacks in both static and mobile sensor networks. In this study, researchers propose an algorithm which is randomized, distributed and dynamically detect the clone nodes and analyses the performances of the existing protocols LSM and RED in terms of detection probability and communication overhead (memory occupation). The main requirements of the distributed algorithm are discussed by Conti *et al*. (2006).

Witness node selection: The witness node may be selected randomly or pseudo-randomly in the distributed network. To predict the witness node either the ID or the location is used.

Overhead: Since, the sensor network is resource-constrained, the overhead in message transmission should be avoided.

For an efficient algorithm, it should be distributed in nature and should select the witness node so as to minimize communication cost and increases the detection probability (Conti *et al*., 2007).

MATERIALS AND METHODS

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 (Xing *et al*., 2008). From the same ID if location information is received is different, clone node is detected (Zhu *et al*., 2012). But this scheme has drawbacks as lot of message

Corresponding Author: C. Geetha, Department of Computer Science and Engineering, RMK Engineering College, Chennai, TN, India

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 (Eschenauer and Gligor, 2002) used for its communication (Brooks *et al*., 2007; Chan *et al*., 2003). 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.

The two main protocols appeared by Parno *et al*. (2005) are distributed solutions. The first scheme, Randomized Multicast (RM), sends the information about its location to direct neighbors and in turn each of these neighbors 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 neighbor 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 as shown in Fig. 1. Each node forwards the claims and saves the claims. For example, a node a and clone a' in the network. Neighbor 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.

Two more schemes are proposed which are Single Deterministic Cell and Parallel Multiple Probabilistic Cells

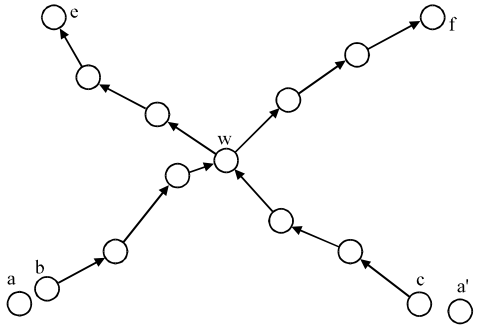

Fig. 1: LSM approach

(Zhu *et al*., 2007). 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 neighbors of a node a send a's claim to these witness nodes with a probability. This solution shows a high detection probability.

Another protocol for detecting node replication attack is SET proposed by Choi *et al*. (2007). A number is generated randomly and it is sent to all nodes and it is used to form disjoint set of clusters and cluster heads. Each cluster is considered as a set and heads of these clusters become leaders of these sets. 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 RED protocol is similar to the RM protocol but with witnesses chosen based on pseudo-random function based on a random value. A random value, rand is generated and distributed to all the nodes using a centralized mechanism. Each node broadcasts a message which contains encrypted ID and location information. The neighbors of source node sends (with probability p) this encrypted message to a set of $g \geq 1$ nodes which are selected using some pseudo-random function (Conti *et al*., 2011). The disadvantage of the RED protocol are number of messages transmitted high, computation time is high witness node is static what researchers fix as $g = 1$, $g \geq 1$, etc. and is location dependent.

Network model and assumptions: In this study, researchers assume nodes are static, non-tamper resistant and are uniformly deployed in the area of observation. Researchers also assume that communication links between sensor nodes are bidirectional (Yu *et al*., 2009) and there is no centralized trusted entity in sensor network. Also, nodes are assigned with a unique ID (Jian *et al*., 2012), prior to their deployment. Assumptions made about the adversary are an adversary can compromise only a limited number of nodes an adversary can take full control over the compromised node an adversary can create as many replicas as adversary wishes to deploy into the network and an adversary cannot create a new ID for sensor node (Ho *et al*., 2009).

Key generation: It provides authentication to node in a network to give security. Algorithm used to generate key is RSA algorithm. The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secures Publickey Encryption Methods (Adleman *et al*., 1977). The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Table 1: Notations used

Variables	Definition
n	Number of nodes in the network
K_a^{priv}	a's private key
dir	Direction chosen by the source node
EM	a's signature on M (encrypted message)
α	Witness node
ID_a	Node identifier of sensor node a
Loc_a	Location of node a

Using an encryption key (e, n), the algorithm is as follows: represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range. Encrypt the message by raising it to the eth power modulo n. The result is a cipher text message C. To decrypt cipher text message C, raise it to another power d modulo n. The encryption key (e, n) is made public. The decryption key (d, n) is kept private by the user.

Prediction: Two types of prediction used in the schemes are ID information and location information. This protocol does not provide any information about ID of the witness nodes during the next iteration of the protocol and also the probability that the witness node selection is not depending on the location of that node. The protocol uses both ID and location information to detect replica in the network.

Notation: For clarity, researchers list the symbols and notation used throughout the study in Table 1.

Proposed system architecture: A source node sends the location information, it randomly selects one direction and to the neighbor node in that direction. This neighbor node randomly/hash function computation, computes a diameter. All the nodes within the circle whose diameter is d will receive the location information and compares. The node within the circle and at the edge or boundary in the same direction becomes the witness node. From this node , the location information is forwarded to a node in randomly selected direction. The proposed system architecture is given in Fig. 2.

The proposed protocol is executed as given: the node a and a' send the location and ID information to a neighbor in the direction selected randomly. This neighbor node computes the diameter and collecting nodes within that diameter and compares the location and ID. If the IDs are same and location is different clone node is detected and it starts the revocation procedure. Otherwise, this information is forwarded to a node on the boundary of the circle or near to the edge. Then the same procedure is repeated until it finds the clone. The proposed protocol steps are given as:

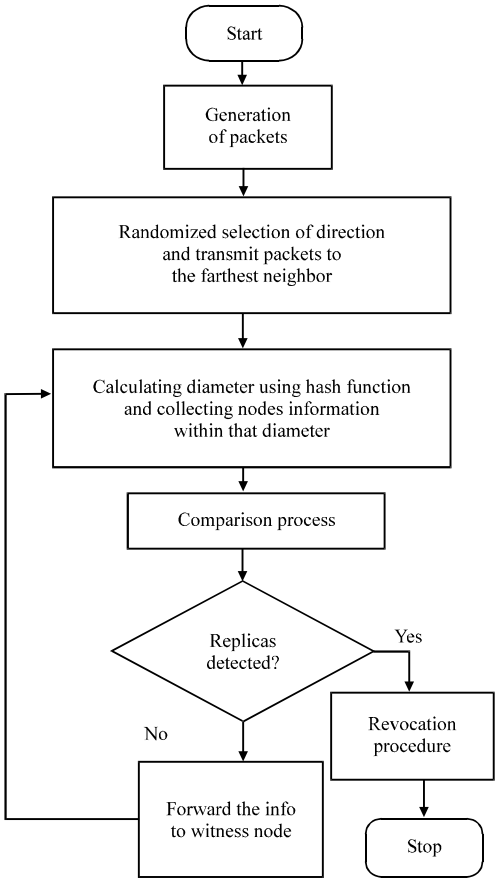

Fig. 2: Proposed system architecture

Input: Encrypted message with ID, location and time.

Output: Detection of clone nodes.

Step 1: Source node a encrypt the message with ID, location and time using RSA algorithm.

Step 2: This encrypted message is sent to a neighbor node which is randomly selected based on the direction.

Step 3: The neighbor node when receives the message, decrypt it using RSA algorithm and check for authorization of the source.

Step 4: If not authorized discard the message.

Step 5: If authorized, compares the ID and location of the received message with the existing one.

Step 6: If IDs are same and different locations clone node is detected and initiate the revocation procedure.

Step 7: Otherwise, the neighbor node compute a diameter using hash function and forward the message to all the nodes within the diameter range.

Step 8: All these nodes perform the comparison and start the revocation procedure if clone node is detected. Otherwise, the farthest neighbor node, a node diameter/2 distance apart in the same direction is selected as a witness node.

Step 9: This witness node repeat the protocol from step 2-8.

X-RED is executed in frequent intervals of time. Every run of the protocol consists of eight steps. In the first step, source node digitally signs its message-ID and geographic location and forwards it to the farthest neighbor in the randomly selected direction. When the neighbor receives the message, it executes step 2-7. The neighbor node computes the diameter and within the circular area from all nodes the location claim is collected and compared. If there is no clone find a witness node is selected as given in step 8. X-RED does not send message to the specific ID. A message sent to a node that is not available in the network would be discarded; nodes deployed after the initial network deployment are not selected as witnesses because need toupdate all the nodes.

Step 1 encrypts a message (claim) and forwards it to the randomly selected neighbor. Generally, message consists of time, ID and location of the source node. Each neighbor receives the message performs the following steps:

- Verifies the received message for its authentication
- Check the message for its freshness

For every valid message that passes this step, the possible witness node extracts the ID and location. If is the first message contains this ID then the node simply stores the message. Otherwise, compute the diameter and collect all neighbor nodes information within that diameter.

If another node with same ID as a source within the diameter has been present, the node checks if the new claim is having different location information than the one stored in memory for this same ID. So, the witness node triggers a revocation procedure for the ID the two signed claims having same ID and different location information are the proof of cloning.

Here is an example of a run of the protocol. Assume that the adversary clones identity ID_a and assigns this identity to nodes a and a'. These two nodes are placed in two different network locations: l1 and l2, respectively. During an X-RED iteration, the nodes a and a' have to broadcast the same ID but different location claims (l1 and l2). Both a and a' starts sending the location information $<ID_a, l1>$ and $<ID_{a'}, l2>$, respectively to their neighbors in a randomly selected direction. Now each neighbor dynamically computes the diameter. Within that diameter area all the nodes will receive this information. But a node on the boundary or near to the boundary will be considered as witness node (w). The same procedure is repeated and at the same time a' will also execute the same protocol. The same w will receive the claim from a and a' and then finds the clone and trigger the revocation procedure.

RESULTS AND DISCUSSION

In this study, researchers show that X-RED meets the following requirements: unaware of ID and location information; less storage overhead and high clone attacks detection probability. Researchers further compare X-RED with RED and LSM and show that X-RED outperforms both RED and LSM in several ways. In the following simulation, researchers fixed n = 1,000 nodes in the network and initially researchers set communication radius as 0.1 (Bettstetter, 2002; Pietro *et al*., 2004). To test the protocols, researchers assume that there are two nodes with the same ID in the network.

The probability that a particular node becomes a witness node is $P_{witness} = 1/m$ where m is the number of nodes for which $l \le d \le l+\varepsilon-1$ (ε: a small value), l: diameter randomly calculated and d: distance between neighbor and witness.

Table 2 shows overheads while message transmission and signature check. Table 3 shows the communication cost and detection probability of various protocols.

Figure 3 the number of messages that are stored by each node in X-RED, LSM and RED. X-axis represents number of messages stored by sensor nodes and Y-axis represents % of the nodes stores fixed number of messages. The graph is obtained by plotting the values taken from the results of >1000 simulations. Note that for LSM (Cho *et al*., 2013), some nodes could require to store

Table 2: Comparison of overheads of LSM, RED and X-RED

Protocol	Communication cost (messages sent and received)	Signature check
LSM	$O(g.p.d.\sqrt{n})$	$O(g.p.d.\sqrt{n})$
RED	$O(g.p.d.\sqrt{n})$	O(g.p.d)
X-RED	$O(g.p.d.\sqrt{n})$ (g = 1)	O(g.p.d) (g = 1)

Table 3: Comparison of communication overhead and detection probability

	LSM		RED		X-RED	
Iterations	CO	DP	CO	DP	CO	DP
5	40	0.35	36	0.840	3.5	0.880
10	20	0.33	10	0.830	7.5	0.870
15	4	0.25	2	0.814	2.0	0.854
20	4	0.72	2	0.130	0.0	0.792

CO: Communication Overhead; DP: Detection Probability

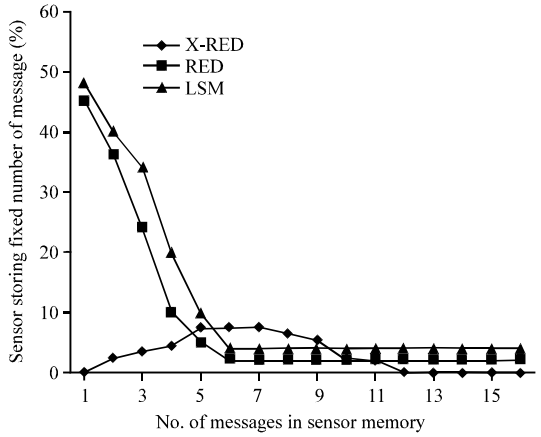

Fig. 3: Messages stored in sensor nodes in LSM, RED and X-RED

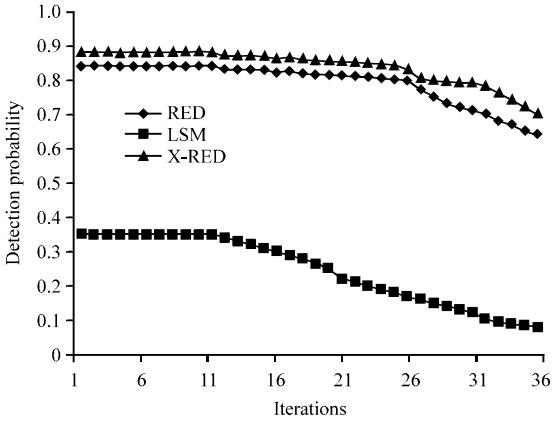

Fig. 4: Detection probability for LSM, RED and X-RED

as many as 200 messages. The experiments show that LSM requires some 60 messages are stored by 1.9% nodes, some 40-59 messages are stored by 7.6% nodes and 27.5% of the nodes store messages between 20 and 39.63% of the nodes are required to store <20 messages. In RED, only a very less number of the nodes store >10 messages (Conti *et al*., 2011). As for X-RED, only few nodes require to store >5 messages which is relatively less than RED (0.001%). The sensor nodes which store the location claim message is very less. In the proposed protocol only the witness nodes are having the capacity of storage. In every iteration, the farthest neighbor in the selected direction is selected as witness.

Figure 4 shows the detection probability in the Y-axis and iterations in the X-axis. The graph is plotted for about 200 iterations. The values were taken from the results obtained for >50 network topology. Each single deployment was evaluated for X-RED, LSM and the RED protocol. For all the iterations, the X-RED protocol shows high probability of detecting clones than RED and LSM. From the 1-50th iteration, LSM shows probability detection of about 35% while this probability is 84% for the RED protocol (Conti *et al*., 2007). However, X-RED shows probability detection of about 85%. When the number of iterations increases, it takes the time to find the clone node and so the detection probability gradually decreases. When compared to the LSM a mass increment in detection probability and compared to RED a slight difference is there but during all iterations X-RED is showing the efficiency.

Analysis of network with malicious nodes: Here, researchers analyze the replica detection probability during a number of continuous iterations. Researchers assume that the malicious node has cloned a node and is already controlling a set of nodes. There is no mechanism for preventing packet dropping and so malicious nodes when it becomes witness node will stop forwarding claim messages. In RED protocol (Zhu *et al*., 2007), the probability that at least one malicious node is present in the two path is:

$$1-\frac{\binom{n-w}{2l}}{\binom{n}{2l}}$$

In X-RED, from both a and a' the claim message is sent to one neighbor node and then to witness node. On the path if there are l nodes, both the paths contain 2l nodes. The probability that atleast one malicious node is present in the two paths is:

$$1-\frac{\binom{n-2}{2l}}{\binom{n}{2l}}$$

CONCLUSION

In this research, three protocols namely LSM, RED and X-RED were discussed for detecting the clone attacks. The proposed X-RED protocol is the major contribution of this research and this research is used to detect node replication attacks and analyzing the performance of all the three protocols. The extensive simulation result shows that the X-RED protocol is highly efficient in detection probability than the existing protocols discussed in the literature. Even though storage overhead is there, it is evenly distributed among the nodes. The advantage of the protocol is to dynamically

compute the direction of the neighbor node, compute the diameter of the area in which all the nodes receive the claim information using hash function and to find the farthest neighbor every time.

REFERENCES

Adleman, L.M., R.L. Rivest and A. Shamir, 1977. Cryptographic communications system and method. U.S. Patent No. 4405829 A. http://www. google. com/ patents/US4405829.

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Networks, 38: 393-422.

Bettstetter, C., 2002. On the minimum node degree and connectivity of a wireless multihop network. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, June 9-11, 2002, Lausanne, Switzerland, pp: 80-91.

Brooks, R.R., P.Y. Govindaraju, M. Pirretti, N. Vijaykrishnan and M.T. Kandemir, 2007. On the detection of clones in sensor networks using random key predistribution. IEEE Trans. Syst. Man Cybernet. C: Appl. Rev., 37: 1246-1258.

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May 11-14, 2003, Berkeley, CA., USA., pp: 197-213.

Cho, K., M. Jo, T. Kwon, H.H. Chen and D.H. Lee, 2013. Classification and experimental analysis for clone detection approaches in wireless sensor networks. IEEE Syst. J., 7: 26-35.

Choi, H., S. Zhu and T.F. La Porta, 2007. SET: Detecting node clones in sensor networks. Proceedings of the 3rd International Conference on Security and Privacy in Communications Networks and the Workshops, September 17-21, 2007, Nice, France, pp: 341-350.

Conti, M., R. Di Pietro, L.V. Mancini and A. Mei, 2006. Requirements and open issues in distributed detection of node identity replicas in WSN. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, October 8-11, 2006, Taipei, Taiwan, pp: 1468-1473.

Conti, M., R. Di Pietro, L.V. Mancini and A. Mei, 2007. Efficient and distributed protocol for the detection of node replication attacks in wireless sensor networks. Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing, September 9-14, 2007, Montreal, Quebec, Canada, pp: 80-89.

Conti, M., R. Di Pietro, L.V. Mancini and A. Mei, 2011. Distributed detection of clone attacks in wireless sensor networks. IEEE Trans. Dependable Secure Comput., 8: 685-698.

Eschenauer, L. and V. D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceedings of the ACM Conference on Computer and Communications Security, November 18-22, 2002, Washington, DC., USA., pp: 41-47.

Ho, J.W., D. Liu, M. Wright and S.K. Das, 2009. Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks. Ad Hoc Networks, 7: 1476-1488.

Jian, H., X. Yan, M.X. Li and F.Y. Miao, 2012. A range-based detection method of replication attacks in wireless sensor networks. Proceedings of the International Conference on Information and Computer Networks, Volume 27, February 26-28, 2012, Singapore.

Lupu, T.G., 2009. Main Types of Attacks in Wireless Sensor Networks. In: Recent Advances in Computer Engineering, Rudas, I. and N. Mastorakis (Eds.). WSEAS Press, USA., pp: 180-185.

Parno, B., A. Perrig and V. Gligor, 2005. Distributed detection of node replication attacks in sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May 8-11, 2005, Oakland, CA., USA., pp: 49-63.

Pietro, R.D., L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, 2004. Connectivity properties of secure wireless sensor networks. Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, October 25-29, 2004, Washington, DC., USA., pp: 53-58.

Xing, K., F. Liu, X. Cheng and D.H.C. Du, 2008. Real-time detection of clone attacks in wireless sensor networks. Proceedings of the 28th International Conference on a Distributed Computing System, June 17-20, 2008, Beijing, China, pp: 3-10.

Yu, C.M., C.S. Lu and S.Y. Kuo, 2009. Efficient and distributed detection of node replication attacks in mobile sensor networks. Proceedings of the IEEE 70th Vehicular Technology Conference Fall, September 20-23, 2009, Anchorage, AK., pp: 1-5.

Zhu, B., V.G.K. Addada, S. Setia, S. Jajodia and S. Roy, 2007. Efficient distributed detection of node replication attacks in sensor networks. Proceedings of the 23rd Annual Computer Security Applications Conference, December 10-14, 2007, Miami Beach, FL., USA., pp: 257-267.

Zhu, W.T., J. Zhou, R.H. Deng and F. Bao, 2012. Detecting node replication attacks in wireless sensor networks: A survey. J. Network Comput. Appl., 35: 1022-1034.