A Distributed Algorithm to Detecting Node Replication Attack in Mobile Wireless Sensor Networks

Samane Mostafaei
Department of Computer Software,
Malayer Branch,
Islamic Azad University,
Malayer, Iran

Keramat Hasani
Department of Computer Software,
Malayer Branch,
Islamic Azad University,
Malayer, Iran

ABSTRACT

One of the dangerous attacks in mobile wireless sensor networks is node replication attack. In this attack, adversary captures one of the network's legitimate nodes and extracts its important information including ID and key materials and uses this information to create duplicate (or replica nodes) and inject them to the network. In this paper, a distributed algorithm based on neighborhood information is proposed for identifying replica nodes in mobile wireless sensor networks. In the proposed algorithm, each node is responsible for handling $\sqrt{N}$ other nodes (N is total number of nodes in the network). Efficiency of the proposed algorithm is evaluated in terms of detection probability, replica nodes and false detection rate. Simulation results show that after 100 traffic monitoring rounds, detection probability of replica nodes is more than 0.95 and false detection rate is less than 4%.

General Terms

Security.

Keywords

Replica attack, mobile wireless sensor networks, neighborhood information.

1. INTRODUCTION

A wireless sensor network (WSN) includes a large number of small sensor nodes, limited and cheap resources which perform a particular task in collaboration. Mobile WSNs have wide applications in military, environment, hygiene, exploration and many other fields. Considering the processing and memory limitations, sensor nodes' energy and wireless communications, establishing security in such networks is a very important and challenging task which has attracted many researchers' attention towards this research field [1].

One of the dangerous attacks in mobile WSNs is replication node attack. In this attack, adversary captures one (or more) legitimate nodes and extracts information of its memory. Then, the adversary uses this information to create duplicate nodes (or replica nodes). Replica nodes exactly consist of the characteristics and information (including ID and locking material) of the captured legitimate node. Thus, they can easily communicate with other legitimate nodes. The adversary deploys these replica nodes in the network and triggers various attacks. For example, the adversary can simply monitor a wide part of network's traffic which pass through replica nodes, deteriorate monitoring operation of sensors by injecting distorted data and disturb common SN protocols including clustering and data aggregation [2, 3].

Many algorithms [4-10] have been proposed so far against replica node attack in static SNs. But these algorithms cannot be employed in Mobiles SNs, because these algorithms are based on locating nodes and sending local claims to witness nodes of the network. Considering continuous movement of nodes in mobile SNs, this mechanism cannot be efficient in such networks.

[11-16] have also proposed algorithms against replica node attack in mobile SNs which have drawbacks including communication overhead, high memory, non-scalability, complex process of detecting replica nodes, requiring node location mechanism and using public keys and digital signatures. Purpose of this paper is to propose a distributed algorithm against replica node attack in mobile WSNs such that it resolves the mentioned drawbacks. Rest of this paper is organized as follows: section 2 reviews previous works. In section 3, system assumptions are presented. The proposed algorithm is presented in section 4. Section 5 presents simulation results. Finally, in section 6, the paper is concluded.

2. RELATED WORK

In [4], four algorithms called Node-To-Network Broadcasting (NBB), Deterministic Multicast (DM), Randomized Multicast (RM) and Line-Selected Multicast (LSM) are proposed which employ public key cryptography. In [5], two other algorithms called Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC) based on localized multicast approach or LM are proposed for detecting replica nodes. These algorithms work in SNs with Grid topology. In [9], another protocol called SET is proposed for detecting replica node. Main idea of this algorithm is adopted from this observation that a SN can be modeled as a set of non-overlapping sub-regions.

In [7], another centralized algorithm called RED is proposed against replication node attack. RED is executed in constant intervals. This algorithm includes two stages. In first stage, random value r is shared among all nodes. This can be done centralized (by a satellite or a base station) or distributed. In second stage (detection stage), each node signs its location claim including ID and geographical location digitally (by private key) and broadcasts it. In [8], RED algorithm [7] is reviewed and its feasibility is explored. In fact, this paper uses analyzes and simulations to show that RED can be implemented in real SNs.

In [9], another protocol against replication node attack is proposed which uses symmetric polynomial to establish pairwise key and uses a group-based deployment model. In this protocol, sensor nodes are extended in separate groups or generations. In [10], an algorithm based on Compressed Sensing is proposed for detecting replica nodes, which is called CSI and it is used in static sensor networks.

In [11] and algorithm for detecting replica nodes in mobile SNs based on sequential probability rate test (SPRT) is proposed. Main idea of algorithm [13], SHD is neighbors' set exchange among mobile nodes and selecting witness nodes for detection operation. In general, SHD detection process is based on sending <ID, neighbor-set> message to nodes which are in their own radio range when executing the protocol and using query methods. Two distributed methods called UTLSE and MTLSE have also been proposed in [13] for detecting replica nodes in mobile SNs. Main idea of these approaches is using this mobility feature: two detector nodes exchange their spatial-temporal claims only when they reach each other. Main idea proposed in [14] is using identity authentication based on direction sign of replica nodes. Another algorithm is proposed in [15] which employ single step communications and node's mobility for detecting replica nodes in mobile SNs.

An algorithm is proposed in [16] which detect replica nodes in mobile SNs using observer nodes. Main idea of this algorithm is to use learning agents and neighborhood information during nodes' mobility in the network for detecting replica nodes. In fact, observer nodes become aware of their current neighbors by considering "Hello" messages broadcasted by nodes during the network life and use this information for detecting replica nodes. This algorithm is considered as the basis algorithm in designing the proposed algorithm and it has been tried to enhance its efficiency.

3. ASSUMPTIONS AND ATTACK MODEL

- Sensor node consists of N sensor nodes which are distributed in a two-dimensional region randomly.
- After broadcasting phase, sensor nodes can move according to mobility models like Random waypoint in the operational environment.
- All nodes have a constant radio range equal to r and are not aware of their spatial location.
- The network is homogenous (all nodes have equal hardware and software facilities)
- Each node has a unique ID.
- In addition, considering mobility of sensor nodes in operational environments nodes should broadcast a "Hello", path request, data transmission and keep alive message periodically. In fact, this operation is one of the mobile SN's requirements so that each node can detect its current neighbors at each moment and establish security keys with them and communicate with them if necessary and create their routing table.
- Last assumption is that replica nodes are mobile in the operational environments like usual nodes and broadcast a "hello", path request, data transmission or keep alive message.

4. THE PROPOSED ALGORITHM

Main idea of the proposed algorithm is to use neighborhood information for detecting replica nodes in mobile wireless sensor networks. The proposed algorithm unlike two basis algorithms is completely distributive and each node can independently detect replica nodes. The proposed algorithm has three phases. In first phase, probability vectors and action vectors of each node are configured and then nodes are deployed in the environment. In second phase, each sensor node updates its probability vector by monitoring its local environment's traffic (neighborhood information). This phase is executed in periodic intervals of t (R rounds). In third phase, each sensor node starts detecting replica nodes according to its probability vector. These three phases are discussed in the following.

4.1 First Phase: Nodes' Configuration

In the proposed algorithm, each sensor node is responsible for observing M other nodes (M<<N). That is, each sensor node monitors activity of M specific nodes. If each node wants to monitor all other nodes, high memory and processing overhead would be imposed on each node. This cannot be efficient considering the limited resources of sensor nodes, especially when there are a large number of nodes in the network. In order to overcome this problem, configuration policy of the proposed algorithm is such that each node is only responsible for monitoring $\mathrm{M} = \sqrt[2]{\mathrm{N}}$ other nodes. Set of nodes u that are being monitored are shown with Lu. In first phase, Lu for each sensor node u is specified and loaded in the memory. Monitor set can be selected randomly or deterministically. Suitable option is the deterministic method which ensures that each node is a member of several monitor sets.

By applying $\mathrm{M} = \sqrt[2]{\mathrm{N}}$ policy and definite selection of monitor sets, it is guarantees that each node v is a member of $\frac{\mathrm{N}\times\sqrt{\mathrm{N}}}{\mathrm{N}} = \sqrt{\mathrm{N}}$ different monitor sets, that is, each node is monitored by $\sqrt{\mathrm{N}}$ other nodes.

Thus, for each sensor node, activation vector (A) and probability vector (P) are initialized according to Equation (1). Action and probability vector of node u are represented by Au and Pu respectively:

$$\mathrm{A_u} = \overbrace{[\mathrm{N_i}, \mathrm{N_j}, \ldots, \mathrm{N_k}]}^{\mathrm{M}} \qquad (1)$$
$$\mathrm{P_u} = \overbrace{\left[\frac{1}{\mathrm{M}}, \frac{1}{\mathrm{M}}, \ldots, \frac{1}{\mathrm{M}}\right]}^{\mathrm{M}}$$

Here, Ni, Nj, …, Nk are IDs of nodes monitored by node u. in fact, each sensor node of the monitor set expresses an action. At the beginning, an equal probability, 1/M is assigned to each action.

Each node selects an action (αi) randomly. This action which is selected by node u, is the monitored node which u expects to be observed in its neighborhood in the next monitoring round.

After finishing configuration operation, nodes are deployed in the network environment randomly and this is the end of first phase.

4.2 Second Phase: Traffic Monitoring

In this phase, nodes collect information required for possible replica nodes in the network in addition to performing usual tasks of the network and mobility in the environment. In fact, all nodes update their probability vector during R monitoring rounds. Information required for updating probability vector of each node are collected according to Hello, path request and other messages issued by direct neighbor (single step) nodes. This phase is performed as follows:

1- Each node u in the ith round of monitoring phase collects its current neighboring nodes (considering Hello messages and …).

2- Node u investigates if action (αi) is available in current neighbors set or not. If node αi is available in current neighbors set, this αi action is awarded according to Equation (2) and itis selected for next monitoring round. Otherwise, if αi node is not in the current neighbors of node u, action αi is fined according to Equation (1) and an action is selected from its actions set for next monitoring round. Action is selected randomly and proportional to probability vector. Thus it is possible that αi is again selected for next monitoring round. In fact, the higher is the probability value of a specific action, the probability that it is selected for the next monitoring round is higher. In Equation (2), parameter *a* is the award and parameter *b* in Equation (3) is the penalty.

$$p_i(k+1) = p_i(k) + a[1 - p_i(k)] \qquad (2)$$
$$p_j(k+1) = (1-a)p_j(k) \qquad \forall j, \quad j \neq i$$

$$p_i(k+1) = (1-b)p_i(k) \qquad (3)$$
$$p_j(k+1) = \frac{b}{r-1} + (1-b)p_j(k) \qquad \forall j, \quad j \neq i$$

3- After t time units are passed and usual tasks of the network are performed, nodes select a random destination and move towards their new destination.

4- Steps 1 to 3 are repeated for R rounds.

When R rounds of monitoring phase are finished, nodes will have the final information for detecting replica nodes. Node with identity v (v is a replica node) in the neighborhood of other legitimate nodes meets with other nodes more than normal (when v is not replicated) due to presence of replica nodes, thus probability value correspondent to action of this node is more than probability of other actions.

According to the proposed award and fine model, probability of normal nodes decreases and probability of replica nodes increases. In third phase, this issue is used for detecting and signing replica nodes.

4.3 Third Phase: Detecting Replica Nodes

When second phase of the proposed algorithm is finished, each node starts detecting replica nodes independently and according to its probability vector. This phase is very simple and cheap. In this phase, each node u first finds largest probability value (say P[i]) in its probability vector and if $P[i] \geq 2 \times \frac{1}{M}$ node u detects that node with ID A[i] is replicated.

5. SIMULATION RESULTS

In this section, efficiency of the proposed algorithm is evaluated through simulation and the obtained results are compared with basis algorithm of [16]. Measurement criteria are as follows:

- Detection probability (Ps): this measure determines the probability of detecting replica nodes using the security algorithm. This criterion is achieved by dividing number of successful executions by total number of executions.
- False Detection Rate: is a percent of non-replica nodes which are detected as replica nodes by a security algorithm incorrectly.

Our simulation model is adopted from the model proposed in basis algorithms and is as follows:

- Network includes N sensor nodes which are distributed in a two-dimensional region of 100*100 m2 randomly.
- Adversary captures legitimate CN=5 and creates S replica of them and casts them in the network.
- Award and fine parameters of the proposed algorithm are set as a=0.001 and b=0.05 respectively.
- Radio range of sensor nodes is considered 10 meters.
- In order to verify the results, each simulation is repeated 100 times and the final result is obtained by averaging these 100 iterations.

Experiment 1: purpose of this experiment is to evaluate effect of monitoring rounds, R, on efficiency of the proposed algorithm and compare the results with the basis algorithm. In this experiment, parameter ω=10 is selected for the observer which are responsible for detecting replica nodes. In the proposed algorithm, all nodes are able to detect replica nodes. In this experiment N and S are considered 100 and 10 respectively, that is, network includes 100 nodes and the adversary creates 10 replicas from captured nodes and casts them in the network. In addition, number of monitoring rounds varies from 50 to 150 and its effect on the proposed algorithm and the basis algorithm is evaluated.

Results of this experiment which are demonstrated in Figure (1) show that probability of detecting replica nodes in the proposed algorithm after 50 monitoring rounds is about 0.85, while this value for basis algorithm is about 0.4. After 150 rounds of monitoring phase, rate of this measure for the proposed algorithm and the basis algorithm is 0.98 and 0.68 respectively. Results of this experiment show that detection speed of the proposed algorithm is much higher than the basis algorithm. Superiority of the proposed algorithm is because this algorithm is completely distributed and each node plays a role in detection operation of the replica nodes (proportional to the monitor set). But the basis algorithm is not distributed and procedure of detecting replica nodes is done by a limited number of control nodes called observer nodes. Therefore, the proposed algorithm detects replica nodes in less number of monitoring rounds with higher probability.

In addition, result of this experiment in figure (2) shows that error rate of the basis algorithm is less than the proposed algorithm. Superiority of the basis algorithm in terms of false detection rate compared to enhancement of the proposed algorithm in probability of detecting replica nodes can be neglected. Superiority of the basis algorithm in terms of false detection rate is that a limited number of nodes are responsible for detecting replica nodes, while in the proposed algorithm all nodes are involved in detecting the replica nodes. Since each node might experience error in detection process, thus in the proposed algorithm, false detection rate is a bit higher than the basis algorithm because all nodes are involved in detection process.

Experiment 2: purpose of this experiment is to evaluate scalability of the proposed algorithm. In this experiment, effect of total number of nodes in the network, N, on efficiency of the proposed algorithm is investigated and the results are compared with the basis algorithm. In this experiment S is considered 10 and number of monitoring rounds for the basis algorithm is considered 350 and 500 while number of monitoring rounds for the proposed algorithm is considered 100. In addition, total number of nodes in the networks is changed from 100 to 300 to see its effect on performance of the proposed algorithms and the basis algorithm. Results are shown in Table (1).

Results of this experiment show that in the basis algorithm, probability of detecting replica nodes decreases by increasing the total number of nodes. But in the proposed algorithm, probability of detecting replica nodes by increasing total number of nodes increases. This is because there are only a limited number of observer nodes in the basis algorithm which are responsible for detecting replica nodes. Thus by increasing total number of nodes, observer nodes will detect replica nodes with delay. But in the proposed algorithm, all nodes are responsible for detecting replica nodes, thus by increasing total number of nodes, detection probability increases also.

Experiment 3: purpose of this experiment is to evaluate effect of number of replicas from each node captured by adversary, S, on performance of the proposed algorithm. In this experiment, total number of nodes are considered N=100. Number of replica nodes varies from 5 to 15 and its effect on the proposed algorithm is evaluated. In addition, obtained results are compared with the basis algorithm. Number of monitoring rounds for the proposed algorithm and the basis algorithm is considered 150 and 350 respectively.

Table (2) shows the results of this experiment. The results show that increasing parameter S increases detection probability of both algorithms, because if there are a lot of replication from a specific node, like u, probability of facing node with u ID in different times and locations increases. Thus probability correspondent to action of node u in probability vectors increases faster. Consequently, probability detection increases. Results also show that changing parameter S does not affect false detection rate of the proposed algorithm and the basis algorithm much.

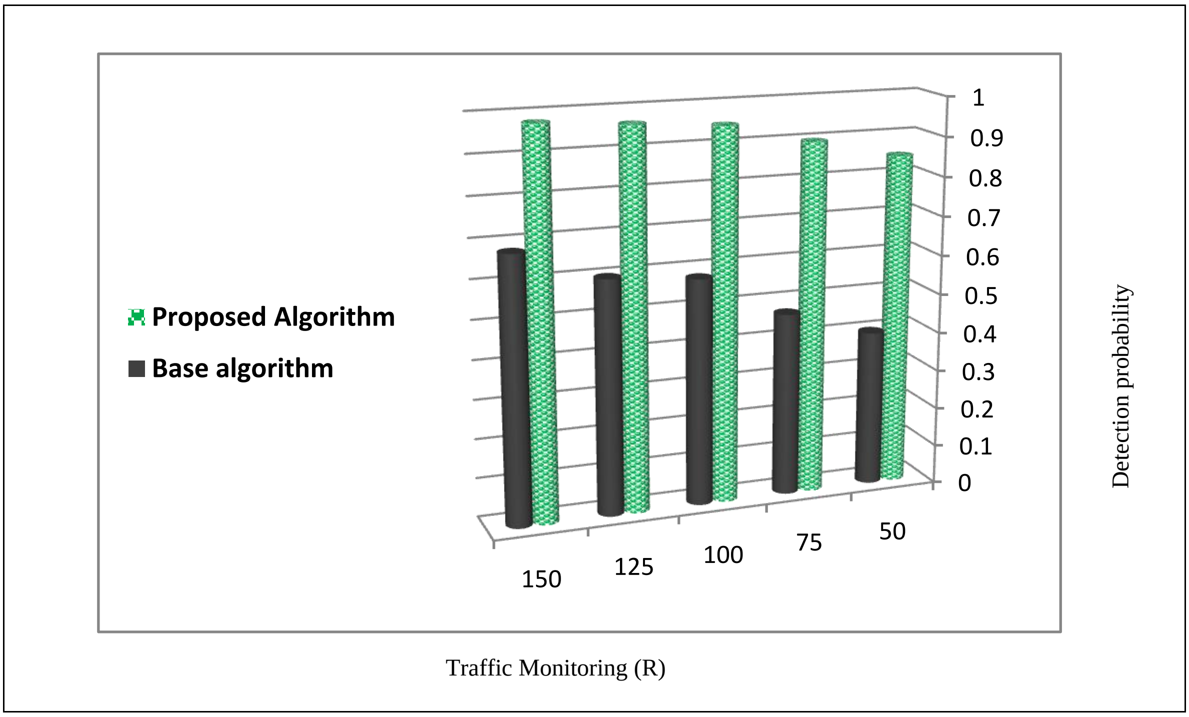

Fig 2. Effect of parameter R on detection probability of the proposed algorithm and comparison with the basis algorithm

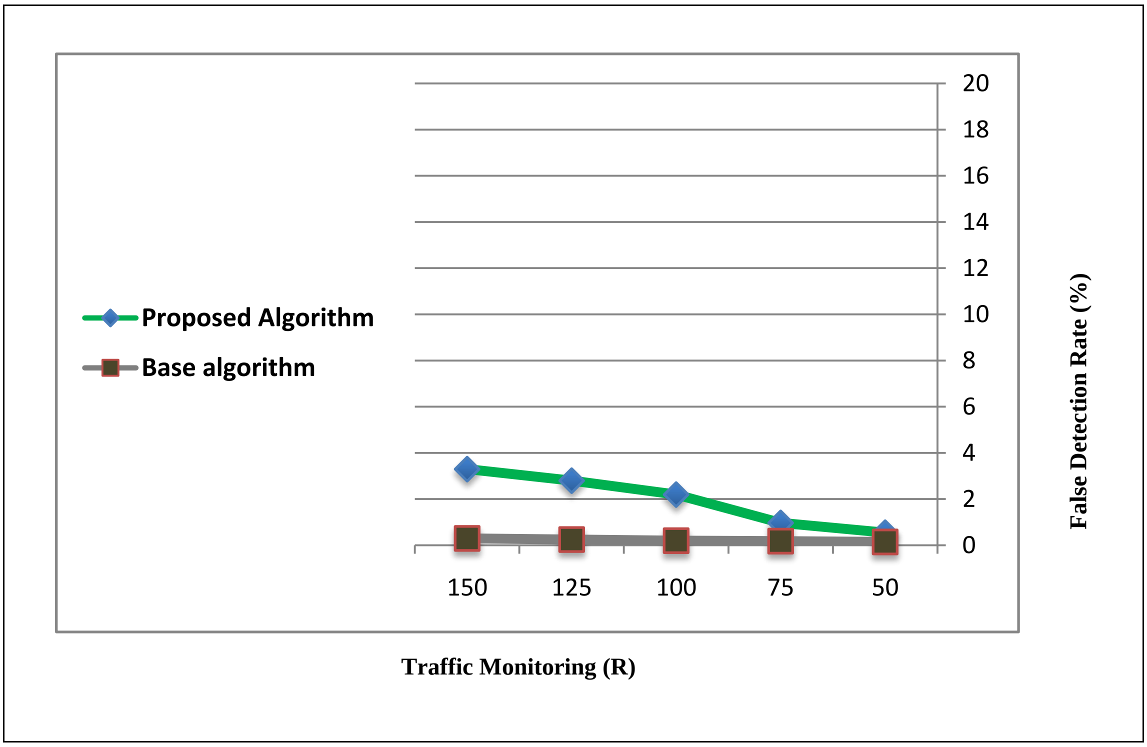

Fig. 3. Effect of parameter R on false detection rate of the proposed algorithm and comparison with the basis algorithm

Table 1. Effect of parameter N on detection probability and false detection probability of the proposed algorithm

	Detection probability			False Detection Rate		
	***N*=100**	***N*=200**	***N*=300**	***N*=100**	***N*=200**	***N*=300**
***Base Algorithm*(*R*=350)**	**100%**	**96%**	**92%**	**0%**	**0.9%**	**1.4%**
***Base Algorithm(R*=500)**	**100%**	**98%**	**94%**	**0%**	**0.5%**	**1 %**
***Proposed Algorithm*(*R*=100)**	**95%**	**99%**	**100%**	**2.3%**	**4.2%**	**4.8%**

Table 2. Effect of parameter S on detection probability and false detection probability of the proposed algorithm

	Detection probability			False Detection Rate		
	S=5	***S*=10**	***S*=15**	**S=5**	***S*=10**	***S*=15**
***Base Algorithm*(*R*=350)**	**70%**	**100%**	**100%**	**1%**	**1.3%**	**1.2%**
***Proposed Algorithm*(*R*=150)**	**85%**	**96.2%**	**98%**	**2.51%**	**2.5%**	**2.6%**

6. CONCLUSION

In this paper, a distributed algorithm for detecting replica nodes in mobile wireless sensor networks is proposed. Main idea of the proposed algorithm is to use an award and fine model based on neighborhood information for detecting replica nodes. Efficiency of the proposed algorithm in terms of detection probability of replica nodes and false detection of rate is measured and the results are compared with the basis algorithm. Comparison results show that performance of the proposed algorithm is better.

7. REFERENCES

[1] Akyildiz I. F., Su W., Sankarasubramaniam Y. and Cayircl E., “A survey on sensor networks”, in: Proceedings of theIEEE Communication Magazine, Vol. 40, pp. 102-114, August 2002.

[2] Akyildiz Ian F. and Kasimoglu Ismail H.,"Wireless sensor and actornetworks: research challenges", in: Proceedings of the Ad Hoc Networks 2, pp. 351–367, 2004.

[3] Anand M., Cronin E., Sherr M. and et al, "SensorNetwork Security: More InterestingThan You Think", in: Proceedings of the USENIX Workshop on Hot Topics in Security, 2006.

[4] Parno B., Perrig A., and Gligor V. D., “Distributed Detection of NodeReplication Attacks in Sensor Networks”, IEEE Symposium on Security and Privacy, 2005.

[5] Zhu B., Addada V. G. K., Setia S., Jajodia S., and Roy S., “EfficientDistributed Detection of Node Replication Attacks in Sensor Networks”,in: Proceedings of the Annual Computer Security Applications Conference (ACSAC), December2007.

[6] Choi H., Zhu S., and Porta T. F., “SET: Detecting Node Clones inSensor Networks”, in: Proceedings of the SecureComm ’07, pages 341–350, 2007.

[7] Conti M., Pietro R. D., and Mancini L. V., “A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks”, in: Proceedings of the ACM MobiHoc, September 2007.

[8] Conti M., Pietro R. D., Mancini L. V., and Mei A., “Distributed Detection of Clone Attacksin Wireless Sensor Networks”, in: Proceedings of the IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING, 2010.

[9] C. Bekara and M. Laurent-Maknavicius, “A new protocol for securingwireless sensor networks against nodes replication attacks”, inWIMOB ’07: Proceedings of the Third IEEE International Conferenceon Wireless and Mobile Computing, Networking and Communications.Washington, DC, USA: IEEE Computer Society, 2007, p. 59.

[10] Yu C.-M., Lu C.-S., Kuo S.-Y., “CSI: Compressed Sensing-Based Clone Identification in Sensor Networks”, in: Proceedings of the 8th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing 2012, Lugano (19 March 2012.

[11] Ho J.-W., Wright M., and Das S., “Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing”, in: Proceedings of the IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 6, JUNE 2011.

[12] Yxainaxniga Y. and et al,” Single Hop Detection of Node Clone Attacks in Mobile Wireless Sensor Networks”, International Workshop on Information and Electronics Engineering (IWIEE), Vol.29, pp. 2798–2803, 2012.

[13] Deng X., Xiong Y., and Chen D., “Mobility-assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks”,In: Proceedings of the6th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2010

[14] Zhu W. T., Zhou J., Robert H. BaoD. F., “Detecting node replication attacks in mobile sensor networks: theory and approaches”, Security and Communication Networks Volume 5, pp. 496–507, 2012.

[15] ContiM., Pietro R. D. and Spognardi A.,“Wireless Sensor Replica Detection in Mobile Environments”, in: Proceedings of the ICDCN, pp. 249-264,2012.

[16] Jamshidi, M., Abbasi, S., Esnaashari, M. and Meybodi, M. R., "A Light algorithm for Detecting the Attacks of Duplicate Nodes in Mobile Wireless Sensor Networks with the aid of learning Agents", Proceedings of 23rd Iranian Conference on Electrical Engineering, Sharif University of Technology, Tehran, Iran, May 10-14, 2015.

[17] Narendra K. S. and Thathachar M. A. L., "Learning automata: An introduction", in: Proceedings of the Prentice Hall, 1989.

[18] Narendra K. S. and Thathachar M. A. L., "Learning automata a survey", in: Proceedings of the IEEE Transactions on Systems, Man and Cybernetics, Vol. 4, no. 4, July 1974.

[19] Narendra K.S. and Viswanathan R., "Learning models using stochastic automata", in: Proceedings of the International Conference of Cybernetics and Society, Washington DC, October 1972.