DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4194

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

RESEARCH PAPER ON DETECTION OF ATTACKS IN STATIC WIRELESS SENSOR NETWORKS

Sapna Juneja
MTech Student
Department of Computer Science
Panipat Institute of Engineering
Panipat, India

Surjeet Singh
Assistant Professor
Department of Computer Science
Panipat Institute of Engineering
Panipat, India

Vikram Bali
Head of Department
Department of Computer Science
Panipat Institute of Engineering
Panipat, India

Abstract:Wireless Sensor Network(WSN) is an accumulation of sensors with constrained resources that work together to accomplish a common objective. WSNs are often installed in harsh environments where because of the unattended nature and lack of tamper proof hardware, an attacker can compromise nodes from the network, and can replicate these captured nodes to many clones using original node's parameters like unique ID and hence, easily gaining control over the whole sensor network.
The proposed clone detection protocol is an efficient approach which easily detects clones in static Wireless Sensor Networks. It is a witness-based approach where some nodes from the network are randomly selected to increase randomness of the network resulting in increased detection probability of the clones. The proposed approach successfully detects the clones which have forged both unique ID as well as location overcoming the shortcomings of existing approach.

Keywords: WSN, Clone, Wireless, Sensor Network, Attack

1. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to observe conditions that are physical or environmental, like temperature, sound, pressure, etc. and to cooperatively pass sensor's information through the network system to a main location (mostly a sink node) [1]. Figure 1.1 below demonstrates an example of a Wireless Sensor Network with sensor nodes relaying sensed information or data to the sink node.

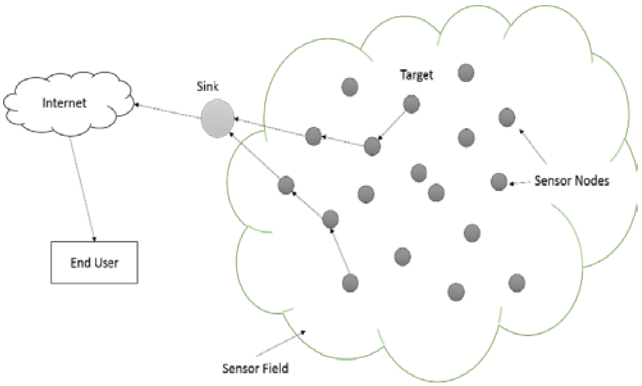


Figure 1.1: Wireless Sensor Network [1]

WSN comprises large number of nodes (thousands or more) which have batteries, sensors, processing units with restricted computation ability, limited memory, and short-ranged radio communication. [7] A node in WSN can be a sensor node or sink node or a Base Station (BS) depending upon their functionality. There are very few sink nodes and a huge number of other sensing nodes.

Sensor nodes use either single-hop long-distance or short-distance multi-hop communication to send data to the sink which leads to single-hop and multi-hop network respectively. The architecture of a multi-hop network is basically categorized into two types: Flat and Hierarchical [16]. In flat architecture, all the sensor nodes have same task responsibilities which act as peers. All sensor nodes present in the network have equal responsibility to carry out different network activities. Each node of the sensor network communicates with the sink node using a multi hop path using its peer nodes as relays. Whereas in hierarchical architecture, clusters are formed with a set of sensors throughout the network. Each cluster comprises a leader called cluster-head. This cluster head is accountable for data flow from cluster members to the sink node.

A. Clone attack

In this clone attack, the attacker may capture a few nodes in the system when they are in threatening environment and concentrate the secret credentials data from nodes, reconstructs or changes the information and makes copies or clones of such nodes in the system. [3] [11] These traded off nodes have impact in system and hence giving the enemy a chance to pick up the control over the system. In this manner security of system had lost and more over these cloned nodes can make more attacks like DoS (Denial of service) inside the network which debases the data. If these clones are left undetected, the network is unshielded to aggressors and in this manner to a great degree helpless.

The rest of the paper has been arranged as follows. Section 2 has provided related research work. Section 3 proposes a random and distributed witness-based clone detection scheme. In section 4, simulation results for the proposed approach have been shown with a brief description about the simulating environment. Finally, section 5 summarizes the work done with conclusion, highlights the contributions of the proposed work and suggests the way for future work possibility.

2. RELATED WORK

Randomized, efficient and distributed approach (RED) [2] [12]: RED (proposed by Conti et al) is a distributed is a distributed protocol to identify clone attacks in Wireless sensor networks. As for the working principal, this protocol is quite identical to already discussed randomized multicast (RM) approach. The difference between both protocols lie in the witness selection

Single deterministic cell approach [15]: This protocol basically involves the selection of witnesses from a specified sub-region of the network. The region zone is determined based on one-way hash function with the input of a node ID and the locations and IDs of all the neighbors of that node are forwarded to this zone.

The neighbors which decides to forward the claim, establish one or more destination cells with the help of geographical hash function [15]. These neighbors bind the sender node's identity uniquely with one or a few of the cells in the specified grid. After this, the generated claim is sent to the determined destination cells utilizing any geographical routing protocol [16].

Here, the geographical hash function [15] is needed to bind identity of a node randomly to a cell in the grid. Whenever a location claim is locally broadcasted by a node, the neighbors both checks the credibility of node's location based on transmission range of the sensor node as well as verifies the claim's signature.

Parallel multiple probabilistic cell (P-MPC) approach: This parallel multiple probabilistic cell approach [14] is basically quite like the single deterministic cell approach discussed above. In this scheme, the information pair (location and ID) is broadcasted to numerous zones. These zones are established just the way they are determined in single deterministic approach.

Just like in SDC scheme, a hash function which is geographical is engaged for the mapping of the identity of a node to the destination cells in P-MPC approach too.

3. PROPOSED METHODOLOGY

A. Attacker Model

The threat model here describes a simple but powerful attacker who can capture some nodes from the network, compromise and replicate them to create clones.

The attacker's main motive is the failure of the clone identification protocol applied to the network and prevent clones from being detected. Hence, to reach this goal, the attacker even tries to detect and ruin the nodes which have the possibility of becoming the witnesses during protocol execution.

Requirement for Detection Protocol

The section presents and justifies the requirements for the proposed witness based detection protocol.

1. Witness Distribution-Major design requirement of the protocol is the selection of witnesses in a way that future determination of witnesses becomes difficult. [9] If the attacker can easily predict the witnesses in next iteration, he can easily corrupt the witness nodes to make the clone attack go undetected. Based on the probability of a node to be a witness, there are two kinds of predictions for the detection protocol:

2 .ID-based prediction – [6] The protocol is considered ID- oblivious if the protocol does not supply with any statistics about the node which will become the witness in the next iteration of protocol.

3. Location-based prediction – [10] A location-oblivious protocol is totally free from location prediction. [8] The witness selection for a protocol run must be independent of location of the nodes within the network. Regardless of its geographical position, witness node can be from anywhere in the whole network.

4. Thus, for the detection protocol to be significantly effective, it should be both ID- oblivious and Location-oblivious as well so that the future witness detection is very difficult even for a smart attacker.

Table 3.1 below describes various notations used in the algorithm to the protocol.

Table 3.1 Notations Used

Notations	Description
IDn	Unique ID for node n
neigh_loc	Location coordinates of neighbor node
T	Timestamp
R	Random number broadcasted at beginning of iteration
G	Witness nodes count for an iteration
L	Node's location coordinates

B. Assumptions

Some basic assumptions made for base station and Wireless sensor network nodes are as follows:

- BS (Base Station) is static in nature and is placed at a considerable distance from the network.
- BS is assumed to be trustworthy and tamper resistant.
- All the sensor nodes are static in nature which means the geographic coordinates of all the network motes are constant.
- A cloned mote is required to involve minimum one uncompromised neighbor.

C. Algorithm

Procedure Receive shows the role of a node as neighbor (received message = claim) or a witness node (received message = fwd_claim). [13] As soon as a neighbor node receives claim message, witnesses are chosen and the claim

is forwarded to the witnesses. The witness is chosen by a pseudorandom function as:

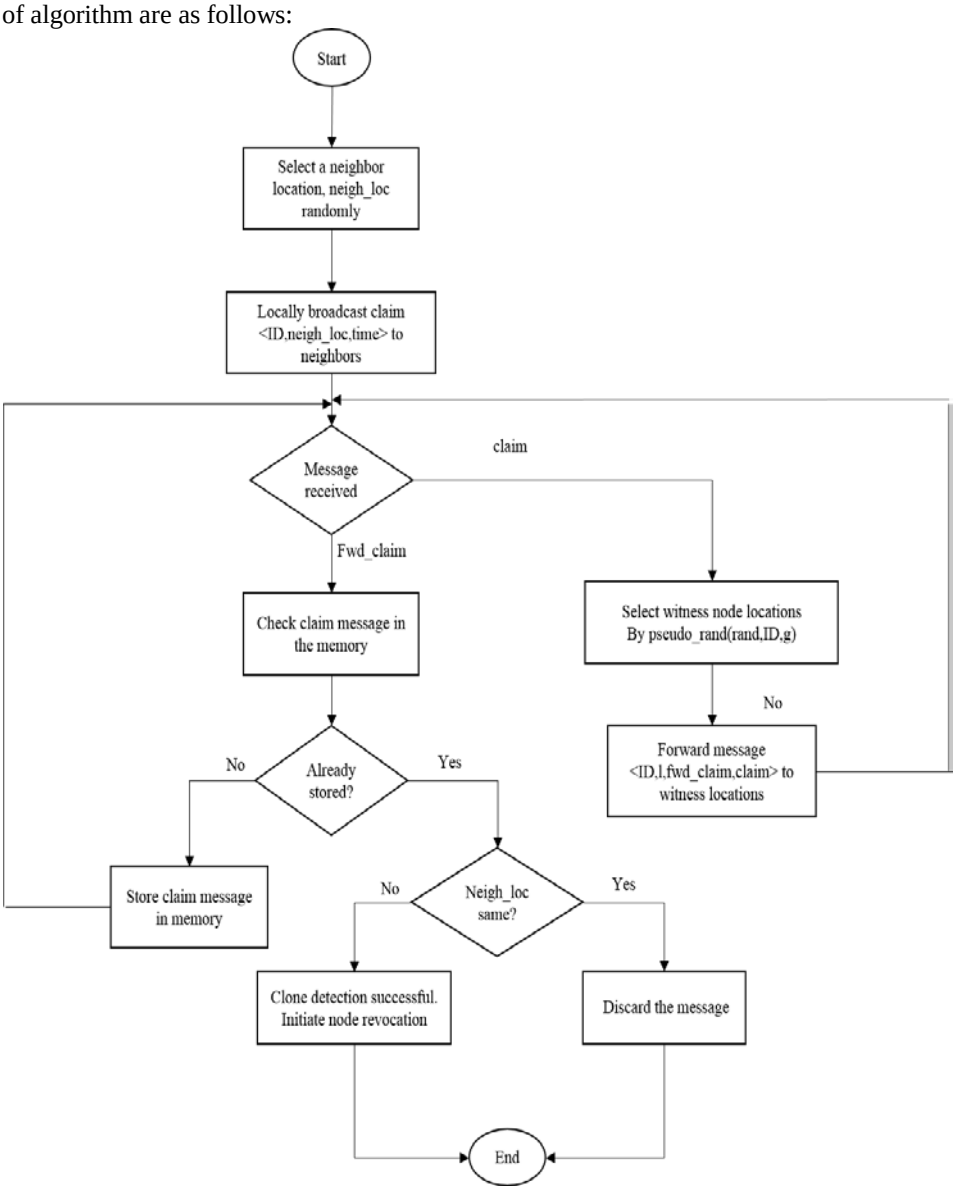
Locations pseudo_rand (IDn, r, g)

The input to this function are ID, r and g which are identity of the original node, the random value and count of witness nodes that are to be generated respectively. The pseudorandom function always provides same output for same set of inputs. Hence for an iteration, a node would always give same set of witness nodes.

The message is then broadcasted towards to the witness nodes which are the possible destinations. Witness, when receives this claim message, acquires the information about location claim from message (neigh_loc and ID here). If this witness node has already encountered any other location claim with redundant ID, the witness examines whether the new claim is same as that of one stored in memory i.e. have same location coordinates or not. [2] If the claim message is coherent with claim already stored in the memory (same neigh_loc), it implies that the message is from original node and hence discarded. If the two claims are incoherent, that node ID is marked as clone.

The revocation of clone includes broadcasting the marked ID as clone to the whole network and blacklisting it from further communication. Steps of algorithm are as follows:

1. Receive broadcasted r value
2. Procedure Claim_Broadcast
3. Select random neigh_loc
4. Claim <Idn, neigh_loc, T>
5. Forward claim to each neighbor
6. End Procedure
7. If received message == claim
8. Locations pseudo_rand (IDn,r,g)
9. For l ϵ locations
10. Forward message <fwd_claim, claim>
11. Else if received message == fwd_claim
12. Check memory for fwd_claim message
13. If already stored for IDn
14. If neigh_loc same for stored message
15. Discard message
16. Else if neigh_loc different
17. clone detected and mark IDn as clone
18. Endif
19. Else store message
20. Endif
21. Endif
22. End procedure



Flow Chart of the Proposed Algorithm

4. SIMULATION STUDY

The section provides detailed description of simulation parameter, methodology and output results through OMNET++ simulator. The simulation deploys 25 sensor nodes within a sample space. The other main characteristic parameters have been defined in the table below.

Table 4.1

Parameters	**Values**
Area	1000×500 m2
Number of nodes	25
Sensor unit radius	40 meters
Number of sink nodes	1
Deployment type	Static
Maximum network packet size	10 bytes

To simulate the real-time wireless sensor network through the simulator, some basic assumptions have been considered. The assumptions made are as follows:

- The sink node and the other sensor nodes are static in nature. They cannot move and change their location once they are deployed in their respective position.
- The attacker can insert clone nodes in the network with some cloned parameters. Clones are assumed to have either ID or both ID and location same as that of the existing node in the network.

The figures 4.6-4.8 below give the output results of the network simulation. In figure 4.6, the initial network deployment has been shown and figure 4.7 describes the message initialization from a sensor node which is broadcasted to its neighbors. Figure 4.8 shows the result where a clone has been detected.

A. Performance Analysis

To illustrate the performance of the proposed approach, 25 nodes have been deployed in the simulation environment. The performance metrics which have been studied here are Detection Probability and Storage Overhead.

Detection Probability-The performance metrics shows the number of successful detection times against total number of simulations. The detection probability metrics assumes both type of nodes, clone nodes with only ID forged and the clones with both ID and location forged. The results for proposed approach are then compared with RED protocol.

Table 4.2: Detection Probability Analysis

Total Nodes	**Clone Nodes**	**Clone Nodes**		**Detection Probability (%)**	
		ID cloned	**ID and location cloned**	**RED**	**Proposed approach**
25	5	3	2	60-62	93-97
25	7	5	2	70-75	94-97
25	10	7	3	68-72	95-98

Table 4.2 compares the detection probability of proposed approach against the RED protocol. Given both type of clone nodes, it is seen that the detection probability of RED protocol approximately lies in the range of 60-70% as the protocol fails to detect the clones which have forged the location too, along with ID. Whereas the detection probability of our proposed algorithm lies somewhere between 93-98%.

Storage overhead-The normal number of messages stored in a single node is taken as a count of memory overhead. Percentage of sensor nodes storing fixed number of messages has been calculated against the number of messages in the memory. The following figure illustrates the memory overhead compared to RED protocol.

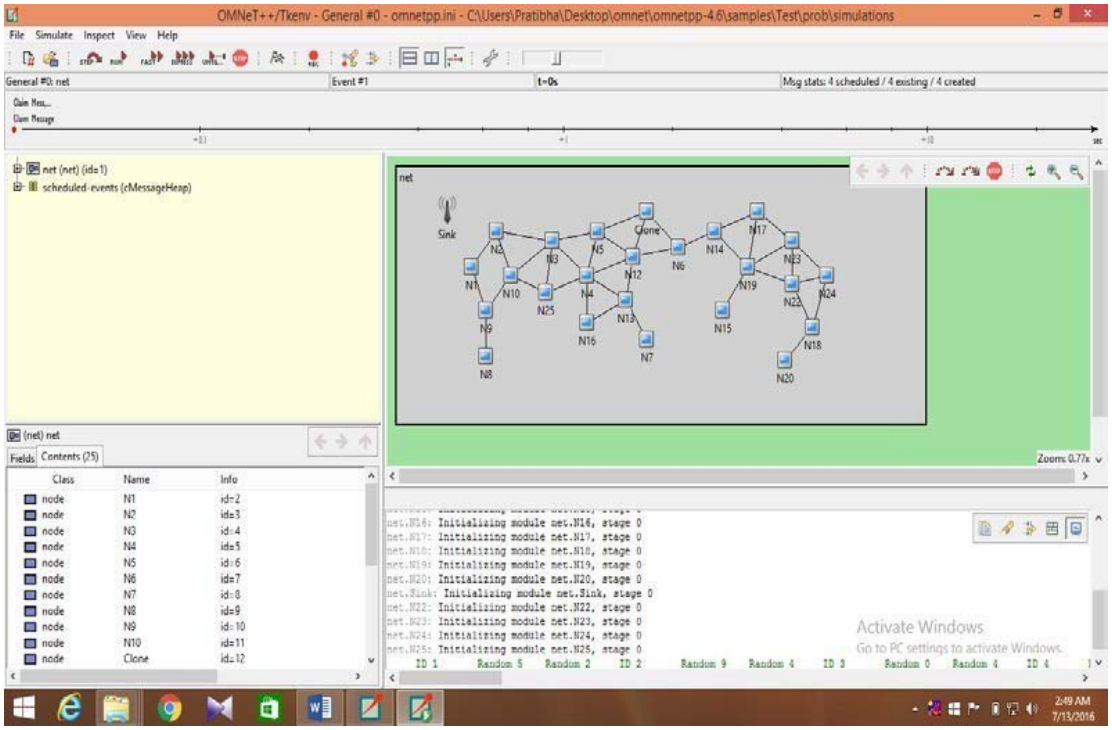


Figure 4.1: Output Results for network Deployment

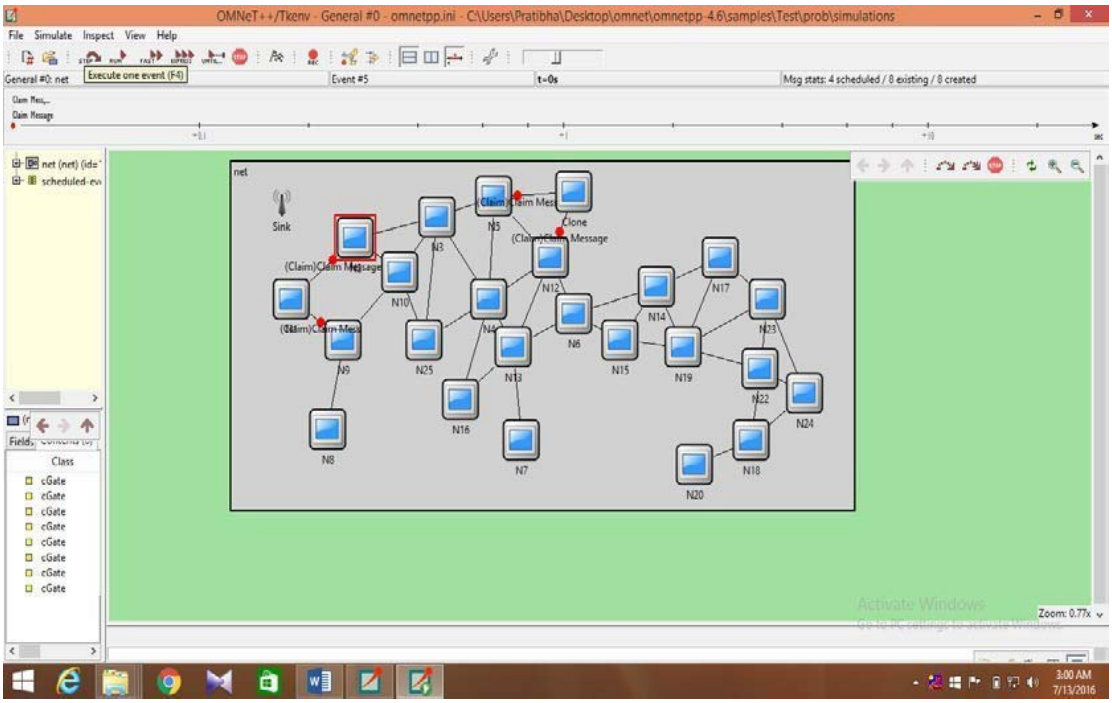


Figure 4.2: Message forwarding

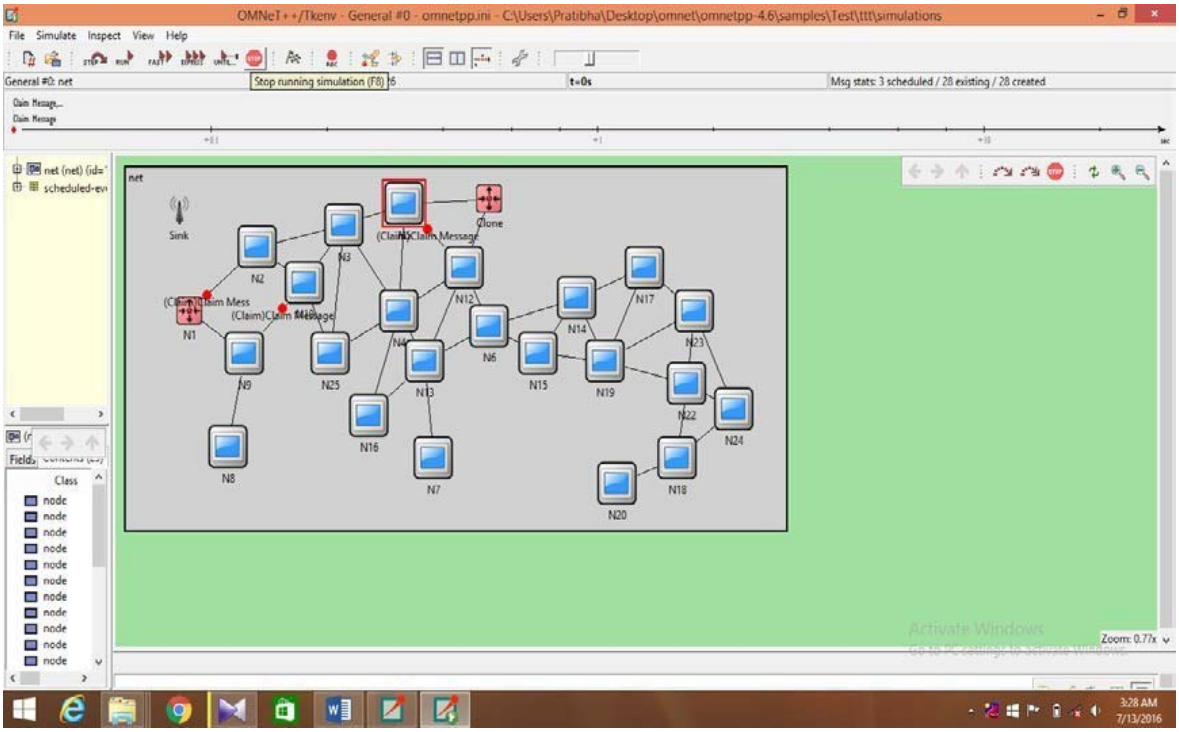


Figure 4.3: Clone Detection Demonstration

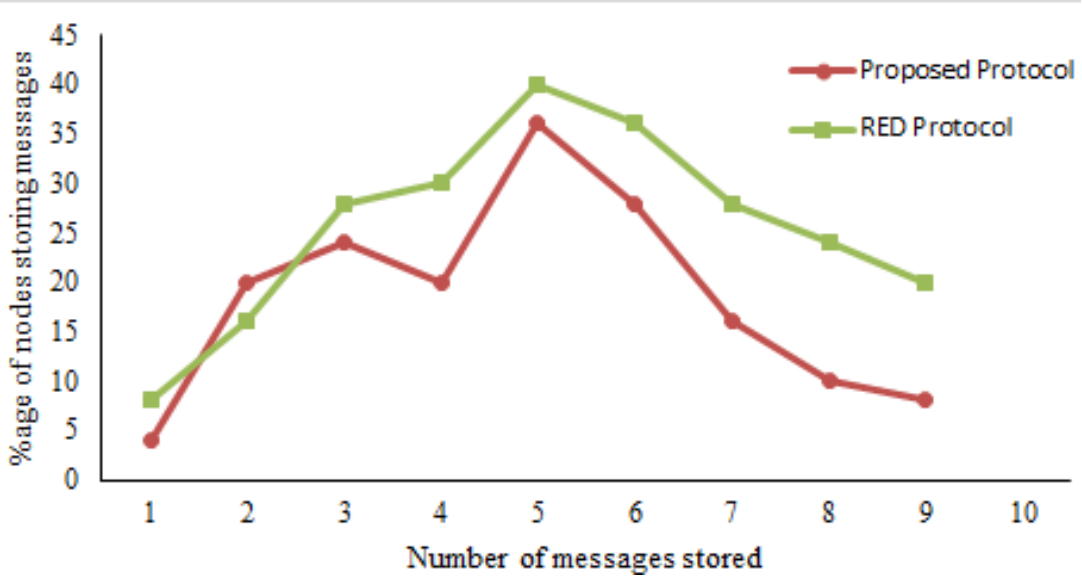


Figure 4.4: Memory Overhead Analysis

5. CONCLUSION AND FUTURE WORK

Real-time WSNs present challenges in terms of privacy, security, mobility, and memory and battery power. Providing security to a WSN is a major concern while deploying the network. Establishing an efficient and stable method for clone attacks is a challenge in static WSN. In this thesis, various defensive approaches (centralized and distributed) for node clone attacks in Static WSN were studied and a distributed witness-based clone detection approach has been proposed. This method helps in spotting the clones throughout the network, even if the location parameter gets duplicated. The proposed witness based clone detection approach is a distributed mechanism to detect clone nodes using randomly selected witness nodes within the network. Messages including ID and neighbor locations are forwarded to witnesses, which then compares it with previously received messages to detect the clone nodes.

The approach proposed in the thesis provides high detection probability and less memory overhead when compared to the existing approaches. The witness based clone detection approach works for the static WSNs that uses randomly selected witness nodes to detect clone nodes in the network. This approach however can be enhanced and used for various other purposes in the future. The approach can be enhanced for mobile Wireless Sensor Networks by considering a node mobility technique. Mobile WSNs need to consider the location factor due to their mobility property.

REFERENCES

1. Archana Bharathidasam and Vijay Anand Sai Pnduru, “Sensor Networks: An Overview”, IEEE International Conference on latest trends in Computer Science, Indonesia, pp. 256-278, October 2010.
2. Conti, R. Di Pietro, L. Mancini and A. Mei, "Distributed Detection of Clone Attacks in Wireless Sensor Networks", IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685-698, 2011.
3. Ruirong Fu, S. Kawamura, Ming Zhang and Liren Zhang, "Replication attack on random key pre-distribution schemes for wireless sensor networks", Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005., 2005.
4. K. Cho, B. Lee and D. Lee, 'Low-Priced and Energy-Efficient Detection of Replicas for Wireless Sensor Networks', IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 5, pp. 454-466, 2014
5. 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
6. C. Cocks, “An Identity Based Encryption Scheme Based on Quadratic Residues,” Proc. IMA Int’l Conf. ’01, pp. 360-363, 2001.
7. Q. Zhang, T. Yu, and P. Ning, “A Framework for Identifying Compromised Nodes in Wireless Sensor Networks,” ACM Trans. Information and System Security, vol. 11, no. 3, pp. 1-37, 2008.
8. M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, “Emergent Properties: Detection. of the Node-Capture Attack in Mobile Wireless Sensor Networks,” Proc. ACM Conf. Wireless Netwok Security (WiSec ’08), pp. 214-219, 2008.
9. J. W. Ho, D. Liu, M. Wright, and S. K. Das, “Distributed detection of Replica node attacks with group deployment knowledge in wireless sensor networks,” Ad Hoc Netw., vol. 7, no. 8, pp. 1476–1488, Nov. 2009.
10. W. Du, L. Fang, and P. Ning, “LAD: Localization anomaly detection for wireless sensor networks,” in Proc. IEEE IPDPS, Apr. 2005, p. 41a.
11. B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, “Localized multicast: Efficient and distributed replica detection in large-scale sensor networks,” IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.
12. K. Cho, M. Jo, T. Kwon, H. Chen and D. Lee, "Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks", IEEE Systems Journal, vol. 7, no. 1, pp. 26-35, 2013.
13. D. Braginsky and D. Estrin. “Rumor routing algorithm for sensor networks”, Proceedings of ACM Workshop on Wireless Sensor Networks and Applications, 2002.
14. A. Fiat and M. Naor. “Broadcast encryption”, In Advances in Cryptology (CRYPTO), 1994.
15. S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan, and S. Shenker, “GHT: A Geographic Hash Table for Data-Centric Storage,” Proc. First ACM Int’l Workshop Wireless Sensor Networks and Applications (WSNA), pp. 78- 87, 2002.
16. Frank L. Lewis, “Wireless Sensor Networks. In Smart Environments: Technologies, Protocols, and Applications”, pages 11 – 46. John Wiley & Sons, 2005.