RESEARCH ARTICLE

Clone Attack Detection Using Pair Access Witness Selection Technique

J. Sybi Cynthia
Research Scholar, C.S.I. Institute of Technology, Thovalai, Tamilnadu, India.
sybi.cynthia@gmail.com

D. Shalini Punithavathani
Principal, Government College of Engineering- Tirunelveli, Tamilnadu, India.
shalini329@gmail.com

Published Online: 03 October 2016

Abstract – Sensor nodes set out in malicious surroundings and are susceptible to pickup and pact. An intruder may reach confidential hidden particulars from these sensors, clone and cleverly spread out them in the network to put up a variety of insider attacks. This attack mode is mostly defined as a clone attack. We propose a new layout for clone attack detection that comes up with successful and well-organized technique called PAWS (Pair Access Witness Selection) technique to detect such clone attacks. Selecting common nodes in between the pairmate as a witness node is the key idea of PAWS to detect clones in the network. The witness selection plays a vital role to overcome the redundancy and reachability problem. The proposed framework results in detecting clones and detection performance depends on the proper selection of witness nodes. Performance analysis and simulations also reveal that our new scheme is more proficient than extant schemes from communication cost and energy consumption.

Index Terms – Clone Attacks, Wireless Sensor Networks, Network Security, Node Replication Detection.

1. INTRODUCTION

Recent technical improvements were able to be local processing and wireless communication in reality that have made the deployment of small, low-cost, low-power, non-centralized devices [1]. The primary components of sensor networks are sensor nodes and it lacks tamper-resistant hardware. This paper focuses on the node replication attack which is also called as clone attack, by which an intruder can compromise any one of the sensor node in the network and fabricate many clones. The clone is nothing but it intrudes into the network with same Identity (ID) of the existing node's ID in different location. The clones are considered to be legitimate members since all credentials are from the compromised node and so it is difficult for making detection easier. On the point of view based on security, the node replication attack has a rigorous impact on networks, since clones are harmful for network operations like key distribution, data collection and routing etc. The technique if detects effectively without a priori knowledge of attack may be the most significant detection technique [2]. Many researches had been exploited in clone attack detection and in most of the existing distributed detection techniques such as LSM [3], RED [4], RDE [5], RAWL [6], ACTIVE [7], SWBC [8] and RTRADP [9], witness-finding strategy plays an important role for identifying the clones where a few nodes in the network act as witness nodes. Undesirably, the communication cost on these methods will be large and thus witness selection is the prime requirement to improve the communication cost and detection performance of clone attack detection scheme. Our proposed Pair Access Witness Selection (PAWS) scheme can identify the clones with better communication cost and energy consumption. By concern with redundancy and reachability, the distributed detection approaches concern with node replication attack was appropriately large in sensor network applications. There are various schemes related to clone attack detection in exist with different parametric evaluations [3] [4] [6] [7] [10]. These techniques try to to pick out the unusual symptom caused by replicas using witness based strategy. But reachability and redundancy problems was not well handled in the existing works.Thus the existing approaches suffers with high communication overhead and energy consumption by requesting redundant information from the network.

Here we evaluate the communication cost and energy consumption as prime performances in our protocol. For excellence, the average number of witness selection by pairing the nodes. Initially this paper concentrates on effective detection of clone attacks by stipulating satisfactory metric such as redundancy and reachability. The proposed work dwell with two phases namely, pairing and witness selection [10] [11]. Each clone attack detection protocol differs by how the witnesses are chosen. First, PAWS securely forms pairing any two nodes in the network. The proposed work concentrates on the witness selection by pairing any two nodes. Secondly, it compares the neighbor list of the pairmate for the common nodes. And only the common nodes from the set of neighbor list were selected as witness nodes. This paper intends strategy techniques for Wireless Sensor Network (WSN) and number of witness node selected to forward the claim. Network Simulator (NS2) is used for implementation and our simulation results bring forth a valuable performance and holds strong resistance against smart attack with significant communication cost and energy consumption for the clone attack detection. The communication cost of our proposed scheme is less than Table-Assisted Random Walk (TRAWL). The left over work is organized as follows. In Section II the previous work was expounded. Then in Section III we elucidate the proposed framework and its techniques. We explicate our numerical results based on analysis in Section IV. To end with we conclude our work in Section V.

2. RELATED WORK

The various protocols deals with the witness based strategy Parno et al. [3] Shares node location information to randomly selected witnesses; extract the birthday paradox for identifying replicated nodes in Randomized Multicast (RM) protocol. In Line Selected Multicast (LSM) protocol, it uses topology as a primary means for detecting replication. It fails to detect nodes that put down or drop messages. As pointed out in Security in Wireless Sensor Network by Broadcasting Location Claims (SWBC) [8] it works by dividing the entire networks into equal angles. The entire network having maximum number of neighbouring nodes selects the root node. Each root node has its witness node to store claim and differentiate the sub nodes and the adversary nodes. It does not concentrate on computational cost.

The Randomized Efficient Distributed (RED) protocol [4] computes the percentage of witnesses towards the total number of witnesses. This protocol is area oblivious. When equal number of node in complete network was compromised, the relevant resilience of LSM is more than RED. The Random Walk (RAWL) protocol [6] surpasses previous approaches because it distributes a core walk by selecting an efficient witness selection and thus an adversary finds difficult to determine vital witness nodes. We tentatively examine the required number of walk steps for certain detection. Clone attack detection scheme was categorized as centralized detection and distributed detection. On focus, the distributed detection was again divided into three various sort of detection based on node to broadcasting, witness based strategy and deployment knowledge. Different existing techniques come under witness based strategy as shown in Figure 1.

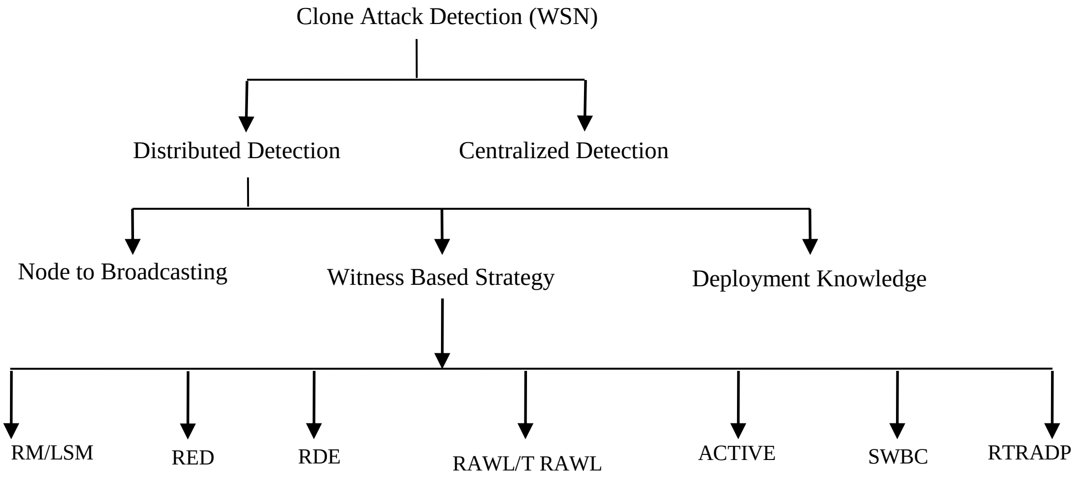

Figure 1 Clone Attack Detection Taxonomy in WSN

Figure 2 shows the clone attack scenario in Wireless Sensor Network. In a network, there are many wireless sensor nodes are available. There occurs a source node, replicated node, collision occurring node and a destination node. If two nodes having same destination address then it confirms clone attack is in the network. The possibility of occurrence of collision is very high.

Most of the time collision occurs while reaching the destination. Melchor *et al*. actively tries each node to learn whether another node is replicated or not eliminating the memory saturation issue. This active approach is that the witnesses scrutinize a set of nodes whose size is independent of node’s count in the network. This result in the same communication complexity than the protocol of Parno *et al.* but no storage is done on the nodes. RDE [5] named Randomly Directed Exploration in which probabilistic directed forwarding scheme is used with border determination. Thus two node clone detection protocols are set up via distributed hash table and randomly explored direction to detect node clones. This protocol obtained that it has good detection probability. Li *et al.* [12] which determines the border reachability. In wireless sensor network, topology plays an efficient role with superior structure [13].

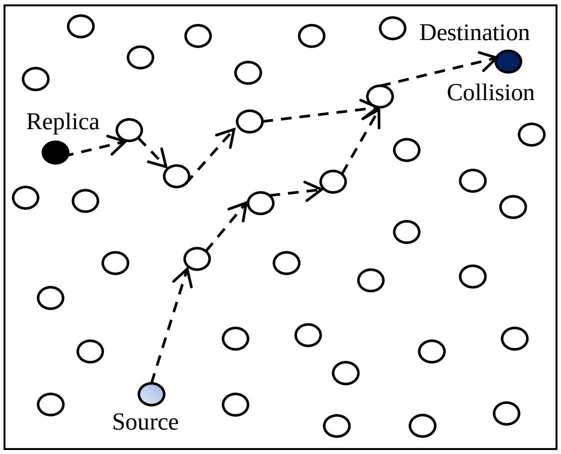

Figure 2 Clone Attack Scenario in Wireless Sensor Network

In Randomized Trust based Replication Attack Detection Protocol (RTRADP) [9] it initialized by giving rise to random seed. It works with witness based techniques that compares with the threshold of the randomly selected nodes. The SET protocol proposed by Choi, Zhu, and Porta [10], carry on to minimize the communication cost of the foregoing scheme by computing exclusive subsets by set operations in the network. SET first launches an exclusive subset maximal independent set algorithm which constructs exclusive unit subsets in a distributed way among one-hop neighbors. Ozdemir *et al.* supports false data detection, the monitoring nodes for each data aggregator also conduct data aggregation and message authentication codes for data verification at their pairmates was computed significantly. The Figure 3 differentiates the witness based strategy in WSN for various existing protocols that comes under clone attack detection. The node replication detection adopts the witness finding strategy [14] and promotes an excellence in cost on detection criteria.

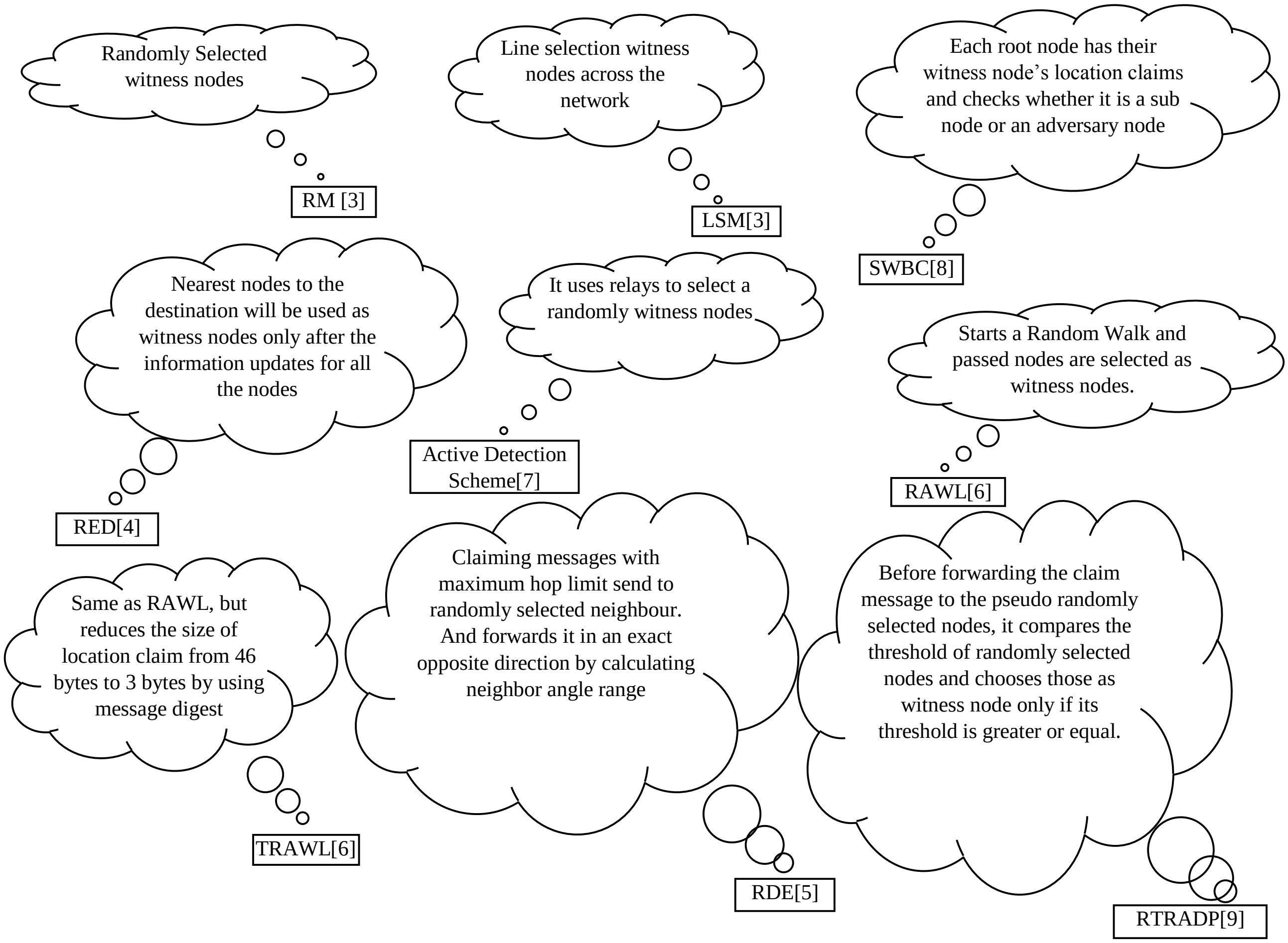
Randomly Selected witness nodes
RM [3]
Line selection witness nodes across the network
LSM[3]
Each root node has their witness node's location claims and checks whether it is a sub node or an adversary node
SWBC[8]
Nearest nodes to the destination will be used as witness nodes only after the information updates for all the nodes
RED[4]
It uses relays to select a randomly witness nodes
Active Detection Scheme[7]
Starts a Random Walk and passed nodes are selected as witness nodes.
RAWL[6]
Same as RAWL, but reduces the size of location claim from 46 bytes to 3 bytes by using message digest
TRAWL[6]
Claiming messages with maximum hop limit send to randomly selected neighbour. And forwards it in an exact opposite direction by calculating neighbor angle range
RDE[5]
Before forwarding the claim message to the pseudo randomly selected nodes, it compares the threshold of randomly selected nodes and chooses those as witness node only if its threshold is greater or equal.
RTRADP[9]

Figure 3 Different Protocols Based On Witness Selection Strategy

3. PROPOSED WORK

Our proposed technique (PAWS) based on witness selection criteria have been presented in this paper. The proposed solution on our clone detection technique concentrates on communication cost and energy consumption. It manages to cut down the communication cost of the foregoing scheme by set operation computation. Firstly, our scheme initiates a subset which forms neighbour list of one-hop. Then it employs to compute set operations and forms the pairmates subset. Secondly, the common nodes from the result of pairmates subset were considered as witness nodes and claims are forwarded to it. Randomization is used to further make the forwarding nodes to be unpredictable to an adversary on witness selection. It purely eliminates redundancy problem during detection. For simplicity, we list the notation used in this paper in Table 1.

Table 1 Notation

n	Number of nodes in the network
g	Number of witness nodes
r	Communication range
r_f	Number of neighboring nodes forward location
e	Energy consumption of each node
h_0	Initial hop count
h_d	Final hop count
N_0	Number of nodes reached

3.1. PAWS Frame Work

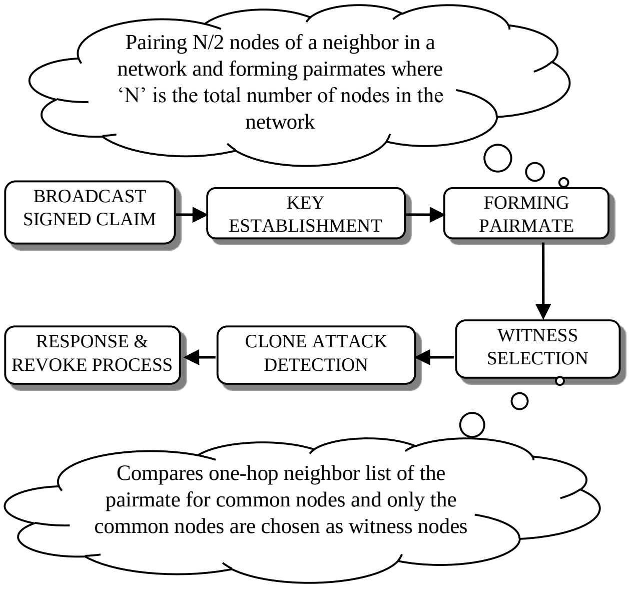
Pairing N/2 nodes of a neighbor in a network and forming pairmates where 'N' is the total number of nodes in the network
BROADCAST SIGNED CLAIM
KEY ESTABLISHMENT
FORMING PAIRMATE
WITNESS SELECTION
CLONE ATTACK DETECTION
RESPONSE & REVOKE PROCESS
Compares one-hop neighbor list of the pairmate for common nodes and only the common nodes are chosen as witness nodes

Figure 4 System Framework – PAWS

Our system framework for the proposed technique (PAWS) was briefly explained in Figure 4. Each node broadcast its claim to its neighbour that includes node's identity and location information. The neighbor node forwards the claim to the witness node. The witness node becomes the evidence of the neighbor's claim. And when the location conflicts for same ID of two nodes, then clone attack was detected in the network. The proper actions should be taken when replica is detected to revoke the node's credentials.

3.2 Proposed Algorithm (PAWS)

3.2.1. Protocol Outline

Individual node broadcasts a signed location claim. Each node updates the list of its neighbor. It pairs the two nodes as a pairmate. Then it compares the pair mate's neighbor list and retrieves the common nodes of the pairmate's neighbor list. Then common witness nodes are selected. And forward location claim to the selected witness nodes. Based on ID of each node and XOR operation was performed during key establishment between the pairmate. Each common nodes computes digest and checks for conflict of location and id. When any one of the witness node gets different location claim for the similar node ID, it means the network was under the attack of clone. Both the nodes having similar id with unique location will be blocked first and revoke process proceeded. Frequent level key change process is done finally.

3.2.2. Pairing Sensor Nodes

A paired node will not be pair set (mate) to other node ie., once the node paired will not be paired with other node and it is unique pair combination. If paired once, it will not be selected again for other to be paired, if energy is less than 50%. The nodes are required to carry on little state information for making routing algorithm simple. In addition, altered routes are chosen for same pair of source and destination nodes at dissimilar time and thus false data injection problem has been overcome. N/2 number of pairs may be formed from N number of nodes in the network. The nearest neighbor is to be paired based on the distance between two nodes and also the energy between the neighbor nodes. The distance of the node can be calculated by the circumference of the antenna power. The prim's algorithm is used to find out the shortest distance concern with energy. The minimum energy limits of a node (e), $e \geq 50\%$. The hop count was calculated by the given formula.

$$\text{Total number of nodes reached} - 1 = \text{hop count}$$

Sensor nodes are randomly deployed in malicious surroundings and are decentralized network. A paired node must be used to transmit data between source and nearest hop. For each session when an event has occurred, the pair mates are selected on the basis of Table 2 and it describes about the energy calculation and the selection of pairmate't' is the threshold energy, E_t is the total energy and e_r is the remaining energy.

To form pairs among sensor nodes, the concerned two nodes give forth a discovery message as “pairmate” including its neighboring node list. The MAC of neighboring node list using the key that shares with the pair node were added along with. Each node that forwards the message appends its ID and location claim to the pair node. When pair node receives, it has the IDs and location claim of its neighboring nodes of pair node. It concatenates the ID of the neighbor nodes randomly and indexes them. Then it computes MAC of the concatenated content and broadcasts the MAC. Hence it is not affect the pairmate election process even if it is compromised. The pair among the nodes is recognized in a related pattern that the pairmates ID’s should be unique.

Table 2 Pairmate Selection

```
d=min(nearestneighbours)

energy=$e_r/E_t$*100

if(d=min&&energy>t=accept)
accept=generateid()
else
reject
endif
end for

generateid()
{
newid=(sourceid)XOR(nearestid)
}
```

3.3. Selection of Witness Nodes among Pairmate

We may get a perception from the SET approach to find the witness nodes by selecting common nodes between pairmate nodes in the network to be accomplished with moderate costs. However our proposed protocol PAWS based on witness selection criteria fulfills the security requirements with reasonable costs. The neighbour list is shown in Figure 5. Our main measure is to employ pair access witness selections which are responsible for identifying the cloned nodes by providing their identities and location as a claim to be forwarded in detection process. The PAWS algorithm briefly explained in the flowchart shown in Figure 6. For selecting witness nodes, we use the set operations intersection scheme to pick out the common nodes between the pairmate to be the best witness nodes set as illustrated in Figure 7. In order to overcome reachability and redundancy problem, the witness selection plays a crucial part in clone attack detection. By selecting the witness node, clone attack detection is performed by monitoring the attitude of the neighbor nodes. The claim was forwarded to the common nodes of a pairmate and it acts as a witness nodes and if conflicts location for the same ID, then it detects or identifies clone in the network. Clone revocation procedure is done immediately after finding clone attack in the network. We acquire better defense against clone attack there by reducing the communication cost and also its energy consumption.

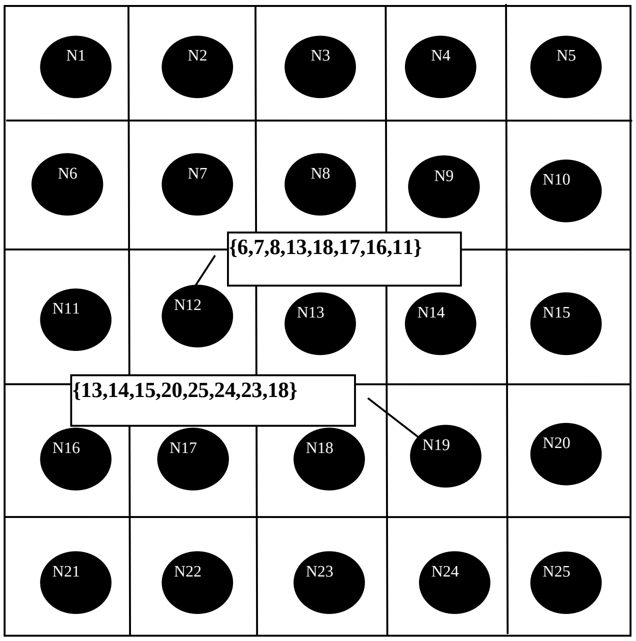

Figure 5 Example Pairmate’s Neighbor List

For a given node, all nodes have equal probability to be as witness nodes. In every execution, for a certain node, nodes having different probability may be as witness nodes. Different protocols vary depending on how witnesses are chosen. Witness walk per node should at least ‘F’ nodes and it should be F > 1. A walk steps ‘W_c” initiated to 1, to a neighbour randomly, it starts a s- step random walk. All nodes have unique identifier in the network. The subset of the sensor nodes is the neighbor list of each node.

The paired nodes’ neighbor lists were compared for common neighbor nodes. For this comparison, it computes intersection of the received subset of the pair mate. The intersection of the subset gives the common nodes out of it and the claim is forwarded only to such common nodes out of two subsets. Thus it overcomes the redundancy and reachability problems instead of forwarding repeatedly to the same neighbor nodes. And thus the energy consumption and communication cost becomes lesser. It employs to compute set operations for finding the common nodes among pairmates and considered as witness nodes to forward the claim for better performance in detection.

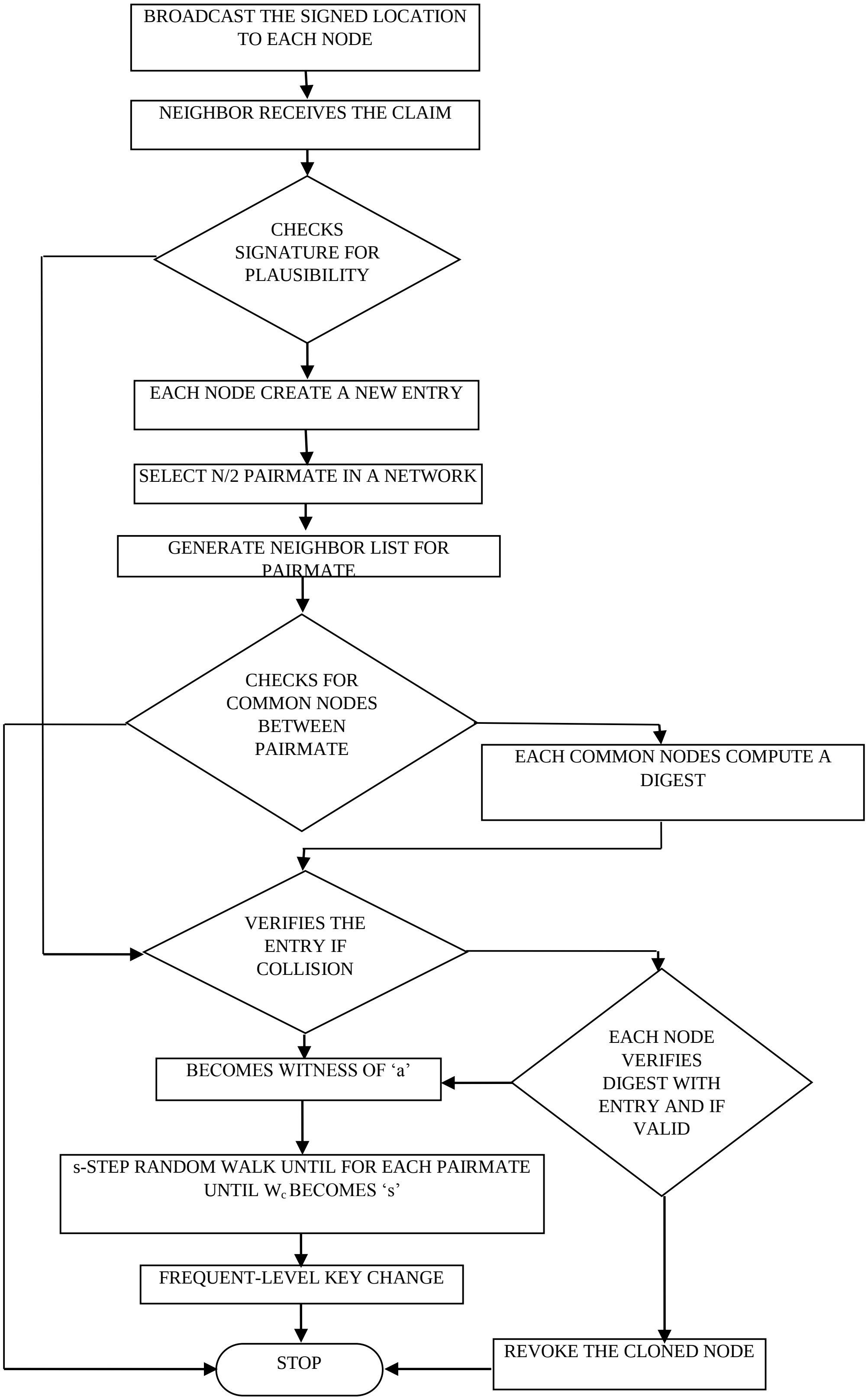
BROADCAST THE SIGNED LOCATION TO EACH NODE
NEIGHBOR RECEIVES THE CLAIM
CHECKS SIGNATURE FOR PLAUSIBILITY
EACH NODE CREATE A NEW ENTRY
SELECT N/2 PAIRMATE IN A NETWORK
GENERATE NEIGHBOR LIST FOR PAIRMATE
CHECKS FOR COMMON NODES BETWEEN PAIRMATE
EACH COMMON NODES COMPUTE A DIGEST
VERIFIES THE ENTRY IF COLLISION
EACH NODE VERIFIES DIGEST WITH ENTRY AND IF VALID
BECOMES WITNESS OF ‘a’
s-STEP RANDOM WALK UNTIL FOR EACH PAIRMATE UNTIL W_c BECOMES ‘s’
FREQUENT-LEVEL KEY CHANGE
STOP
REVOKE THE CLONED NODE

Figure 6 Flowchart – PAWS Algorithm

RESEARCH ARTICLE

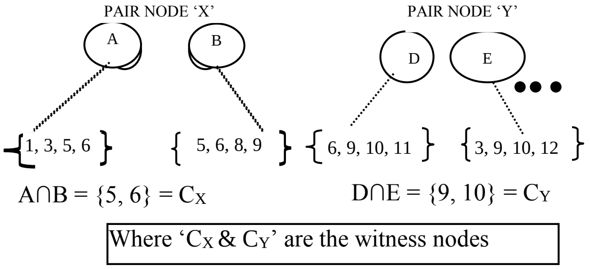

Figure 7 SET Operations for Finding Common

4. EXPERIMENTAL EVALUATION

The simulation parameters and metrics for measuring the network performance are discussed in this section.

4.1. Simulation Environment

We chose NS2 simulation and the simulation setup in an area of 800 X 800 meters with set of 32 nodes. The performance of the network is measured using the metrics namely, communication overhead and energy consumption. Figure 8 shows the simulation result of pairmate and common nodes generation and Figure 9 shows the communication establishment between pairmate and common nodes. Figure 10 shows the data transmission between pairmate and common nodes and Figure 11 shows the source to destination data transmission and thus reachability occurs.

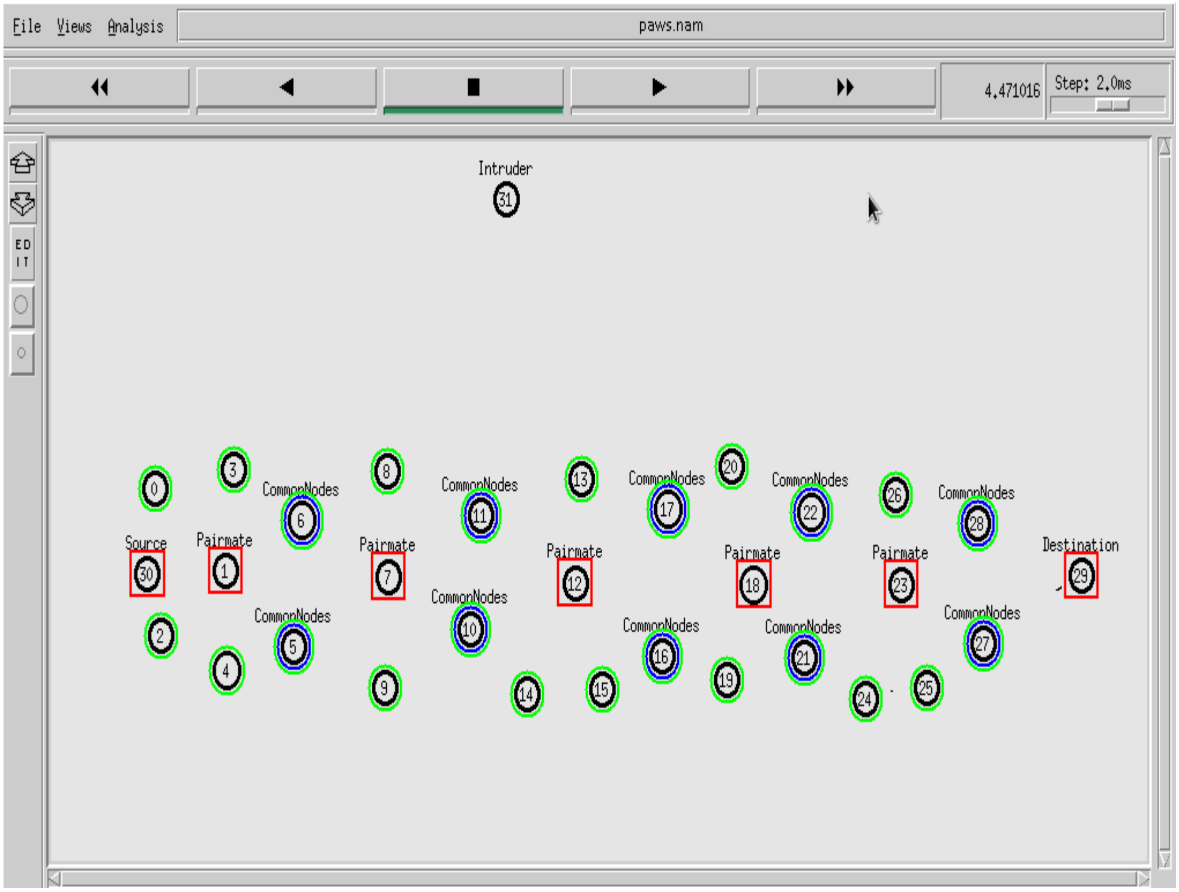

Figure 8 Pairmate and Common Nodes Generation

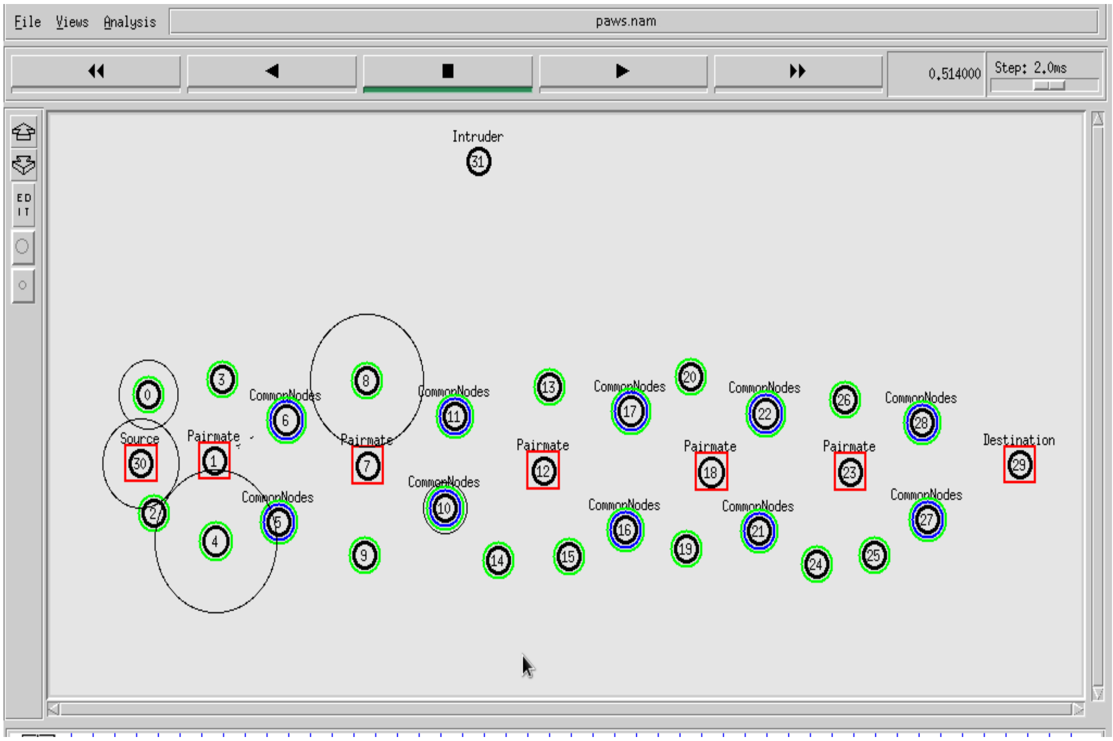

Figure 9 Communication Establishment between Pairmate and Common Nodes

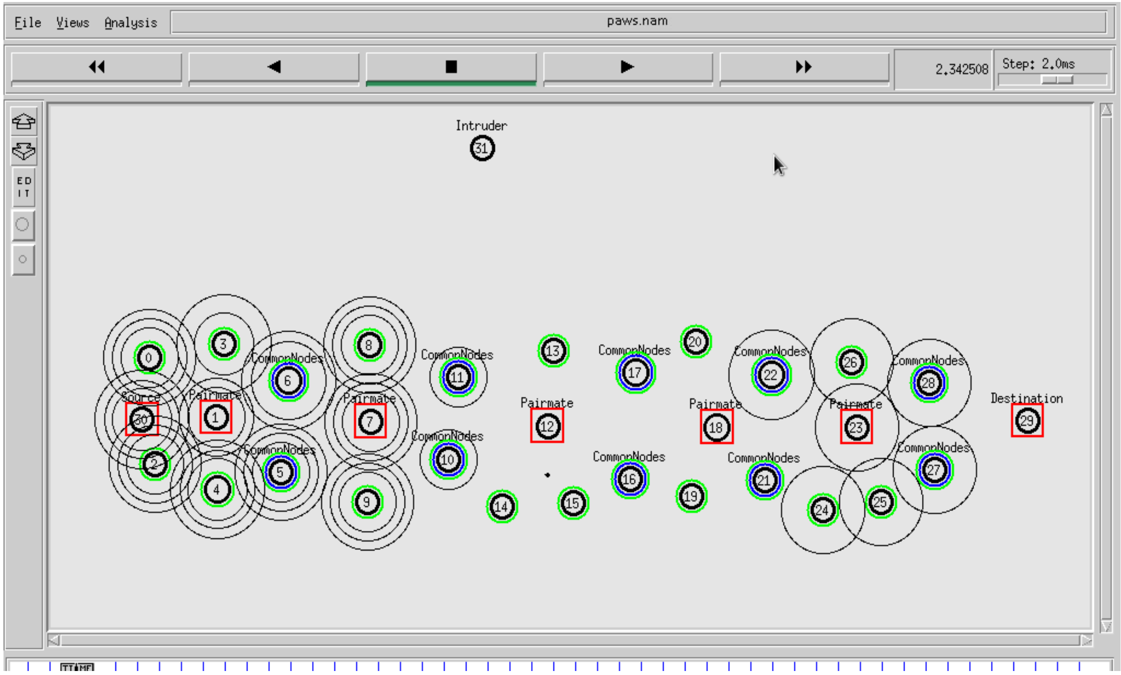

Figure 10 Data Transmission between Pairmate and Common Nodes

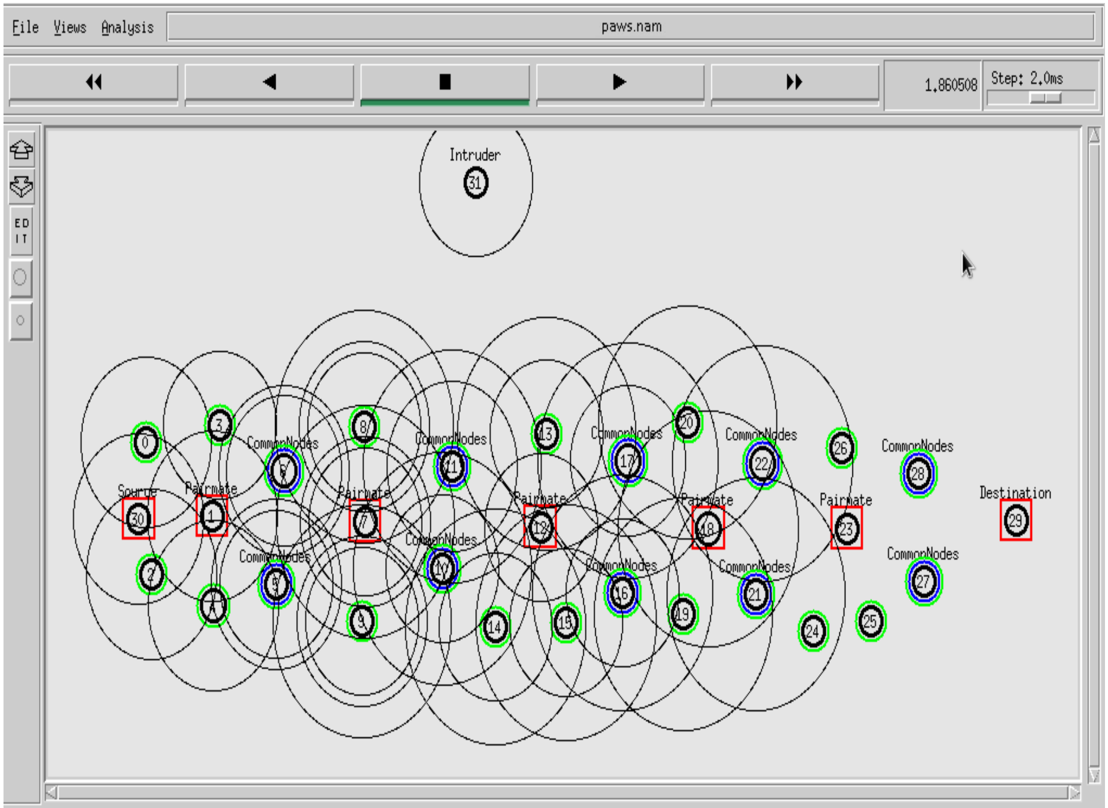

Figure 11 Data Transmission-Source to Destination–Reachability Occurs

4.2. Communication Overhead

PAWS have very low communication overhead as shown in Figure 12. The general requirement of PAWS is that the overhead generated by the protocol should be minimum of it should be sustainable by the WSN as a whole, and evenly shared among all the nodes. Since the pairmate's common nodes was selected as a witness nodes in our proposed work, the communication overhead for PAWS is only less than 50% whereas when TRAWL has an overhead is more than 50%.

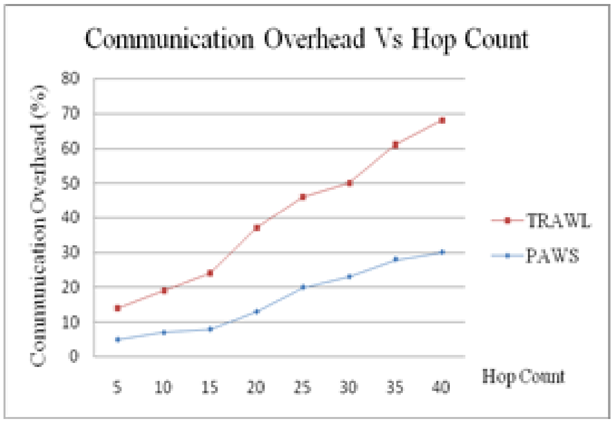

Figure 12Comparison of Communication Overhead

4.3. Energy Consumption

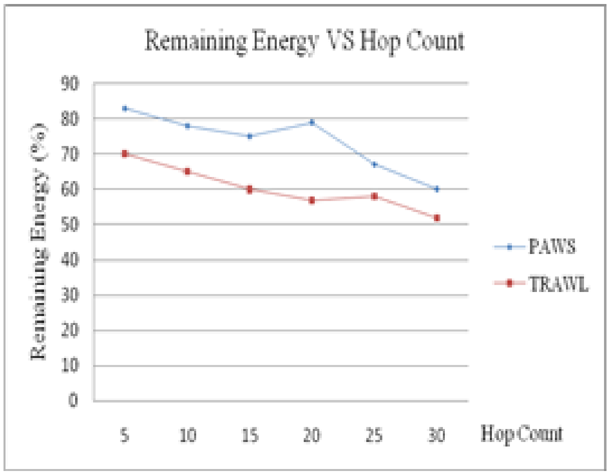

Figure 13Comparison of Energy Consumption

Figure 13 shows that PAWS consumes less energy when compared common nodes and uncommon nodes selected as a witness selection. The proposed work uses message digest in forwarding the claim and it consumes less energy when compared to the existing related work. The energy consume in

PAWS is 10% to 30% for less than 32 hops counts with selecting common nodes as a witness nodes within pairmate whereas TRAWL consume energy of about 30% to 50% within 32 hop counts. The common nodes from the pair mate's neighbor list for the selection of the witness will be more efficient when compared with the uncommon nodes. The communication cost and energy consumption made better performance by choosing common nodes as witness nodes in PAWS.

Table 3 Performance Comparison of Different Protocols

Sl.no.	Protocol	Communication Cost	Memory Cost	Performance Analysis	Performance Evaluation	Reachability	Redundancy Problem considered
1.	LSM	$O(\sqrt{n})$	$O(\sqrt{n})$	By using time synchronization enhancement, storage requirement were reduced.	Probability of detection and Resiliency	Moderate	Yes
2.	RED	$O(\sqrt{n})$	$O(1)$	Memory, communication and computation cost is highly efficient. It improves detection capability since it is ID/Area oblivious.	Energy consumption and Detection probability	Strong	Yes
3.	ACTIVE	$O(\sqrt{n})$	$O(1)$	Witness nodes in the network are reduced. Number of scrutinized nodes per node is constant and thus memory usage also reduced. Communication overhead reduced since no need of clever distribution of relay choice. The detection rate increases.	Detection rate	Moderate	Yes
4.	TRAWL	$O(\sqrt{n}logn)$	$O(1)^2$	Less Communication cost and since torus structure, high probability detection is possible and due to the usage of claim digest, memory cost is less. The security properties are better.	Probability of detection and Resiliency	Strong	Yes
5.	Proposed PAWS	$O(\sqrt[3]{n}logn)$	$O(1)^2$	Reachability occurs since the common nodes were selected for witness. Once selected witness nodes will not be selected	Energy consumption, Detection probability and resiliency	Very Strong	Limited Redundancy

4.4. Discussion

The Witness selections in clone detection technique cause to overcome the redundancy and reachability problems. Energy aware routing scheme is more efficient. Energy consumption is decreased or increased depends on number of hop counts [15]. The number of hops in our PAWS is less when compared with TRAWL. Almost certainly communication cost depends on the selection of witness nodes. Clever distribution of witness path may reduce communication overhead. The comparison of performance analysis and evaluation between existing protocol and the proposed PAWS protocol were explained in Table 3. Node mobility is more challenging for energy conservation in computing. Our proposed will be more efficient in case of reachability since N/2 nodes will be paired and reaches the common nodes of each paired subset in the network where else TRAWL technique never uses pairing concept. Hence reachability in TRAWL is only moderate than PAWS. Here we discuss reasonable implementations of our protocols.

5. CONCLUSION

Using the elegant, efficient technique for detection of clone attack in the network, high remarkable communication cost and energy consumption can be achieved. Several drawbacks in existing solutions related to clone attack detection and a prompt witness selection technique must be required to attain a better performance. One of the existing protocols, TRAWL has high energy consumption and has reachability problem. Our PAWS result shows the improvements in case of redundancy and reachability problems in the proposed technique. By comparing existing unpaired nodes for witness selection scheme, our proposed PAWS technique reduces the cost of communication and also yields wide energy consumption in clone attack detection in the wireless sensor network. PAWS protocol implemented in static WSN but it is beneficial to utilize in mobile network also. In future, fuzzy logic may be applied to improve the detection performance.

REFERENCES

[1] Bharathidasan, Archana, and Vijay Anand Sai Ponduru. "Sensor networks: An overview." In IEEE INFOCOM, vol. 4. 2002.

[2] Baykara, M., Daş, R., "A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems", International Journal of Computer Networks and Applications (IJCNA), 2(5), 203-211, 2015

[3] Parno, Bryan, Adrian Perrig, and Virgil Gligor. "Distributed detection of node replication attacks in sensor networks." In 2005 IEEE Symposium on Security and Privacy (S&P'05), pp. 49-63. IEEE, 2005.

[4] Conti, Mauro, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei. "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks." In Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing, pp. 80-89. ACM, 2007.

[5] Li, Zhijun, and Guang Gong. "Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks." In 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, pp. 1030-1035. IEEE, 2009.

[6] Zeng, Yingpei, Jiannong Cao, Shigeng Zhang, Shanqing Guo, and Li Xie. "Random-walk based approach to detect clone attacks in wireless sensor networks." IEEE Journal on selected areas in communications 28, no. 5: 677-691, (2010).

[7] Melchor, Carlos Aguilar, Boussad Ait-salem, and Karim Tamine. "Active detection of node replication attacks." In International Journal of Computer Science and Network Security (IJCSNS), 9: 13–21. 2009.

[8] Meenatchi, S., C. Navaneethan, N. Sivakumar, P. Thanapal, And J. Prabhu. "Swbc-Security In Wireless Sensor Networks By Broadcasting Location Claims." Journal of Theoretical and Applied Information Technology 64, no. 1, 2014.

[9] Manjula, V., and C. Chellappan. "Trust based node replication attack detection protocol for wireless sensor networks." Journal of Computer Science 8, no. 11 : 1880, 2012.

[10] Choi, Heesook, Sencun Zhu, and Thomas F. La Porta. "SET: Detecting node clones in sensor networks." In Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on, pp. 341-350. IEEE, 2007.

[11] Ozdemir, Suat, and Hasan Çam. "Integration of false data detection with data aggregation and confidential transmission in wireless sensor networks."IEEE/ACM Transactions on Networking (TON) 18, no. 3: 736-749, 2010.

[12] Li, Zhijun, and Guang Gong. "On the node clone detection in wireless sensor networks." IEEE/ACM transactions on networking 21, no. 6 : 1799-1811, 2013.

[13] Manjula, V., and Dr C. Chellappan. "Replication attack mitigations for static and mobile WSN." arXiv preprinarXiv:1103.3378, 2011.

[14] Vançin, Sercan, and Ebubekir Erdem. "Design and Simulation of Wireless Sensor Network Topologies Using the ZigBee Standard." International Journal of Computer Networks and Applications (IJCNA) 2, no. 3: 135-143, 2015.

[15] Merlyn, A. Anuba, and A. Anuja Merlyn. "Energy Efficient Routing (EER) For Reducing Congestion and Time Delay in Wireless Sensor Network."International Journal of Computer Networks and Applications 1, no. 1 : 1-10, 2014.

Authors

J. Sybi Cynthia completed Diploma in Electronics & Communication Engineering in 1997 and she has completed Bachelor of Computer Applications in 2005. She then completed her Master of Computer Applications in 2009 Madurai Kamaraj University, Madurai. She completed her Master of Engineering in Computer Science and Engineering, in 2012 from The Rajaas Engineering College, Tirunelveli, India affiliated to Anna University, Chennai. She is a Part time Research Scholar under Manonmaniam Sundaranar University Tirunelveli; she is currently doing the research in Network Security. Her main interest and work areas are Network Security and Wireless Sensor Network.

D. Shalini Punithavathani completed her Bachelor of Science, in 1979 in Sarah Tucker College, Tirunelveli, India affiliated to Madurai Kamarajar University, Tirunelveli, India. She completed her Bachelor of Technology in Electronics, in 1982 from Madras Institute of Technology, Chennai, India affiliated to Anna University, Chennai, India. She completed her Master of Engineering in Computer Science and Engineering, in 1990 from Government College of Technology, Coimbatore, India affiliated to Bharathiar University, Coimbatore, India. She completed her Doctorate in Philosophy, entitled “Study and Implementation of IPv4 to IPv6 translation techniques” in 2010 in Anna University, Chennai, India. She is working as a Principal in Government College of Engineering, Tirunelveli, Tamil Nadu. Her main interest and work areas are mobile computing and Networking.