Exploration of Attacks Originate by Clone Node in Wireless Sensor Network

Sachin Lalar, Shashi Bhushan, Surender

***Abstract**: Wireless sensor networks are used today in numerous applications. Due to the limited battery, storage and processing power, the sensor node absorbs the environment and sends data to the base station. Wireless sensor networks are vulnerable to various attacks due to their limited functionality. Clone node is the attack where adversary physically grabs the node from its location & generates various nodes by using secret information and reflects them on the network. Due to node cloning, various attacks can easily occur in WSN. In this paper, we describe the layer by layer attacks generated by the clone node in WSN. We compare the network scenarios in Network Simulator 2 in which first scenario are normal network & second scenario has the clone nodes which produce the attack inside network. We estimate the impact of clone node in form of packet loss and also compare packet loss rate in normal network and clone node containing network in 8 different scenarios.*

***Keywords** : Wireless Sensor Network, Attacks, Clone Node Attack, Packet loss.*

I. INTRODUCTION

A wireless sensor network (WSN) consists of small sensor nodes with limited memory, limited power, and processors. The sensor nodes are classified in terms of node-based and sink-node [1]. The nodes which sense the environment and collect the data are known as node-based sensor. The base sensor collects entire data from the node sensors and processes it. The transmissions of data between the sensor nodes are feasible via radio signals. WSN deploy in harsh and open environment, including environmental surveillance, military, building monitoring, health etc where there is high possibility that a security threat will occur [2]. Also due to limited capability of sensor node, it is possible for attacker to attack on WSN with different ways. Some of attacks are selective forwarding, worm hole, black hole, Clone node attack, Hello Floods etc. The clone node attack one of the attacks which can be launched by attacker. In this attack, attacker steals the legitimate sensor nodes from network and obtains the confidential information from sensor node. After extracting the data, invader is able to replicate the node and deploy back in the network [1]. By using these nodes the attacker easily launches other attacks and degrades the performance of wsn.

The purpose of paper is to find out the various attacks that are caused by the clone node in sensor network and analyze the influence of replication attack in the network. We explain the influence of replication attack in form of packet loss. The paper is structured in five sections as: The 2nd Section illustrates the Clone Node Attack. After that the Section 3rd describes various attacks in wsn that are caused by the clone node. Section 4 simulates the clone node attack in ns2 and discusses the influence of clone attack in wsn. The last section presents the conclusion.

II. CLONE NODE ATTACK

An attacker first steals the legitimate nodes from the network in clone node attack, then extracts the sensitive information including key from the captured nodes. Then attacker makes the various copy of that node by using the extract information and put back them in the network. The clone node also called replicate attack. By using replicate attacks, the attacker can easily launch various attacks such as sink hole, selective forwarding, Hello Floods attacks etc [4]. With replication attack, the clone node can control the whole network and may affect the working of network. The attacks also degrade the performance of network.

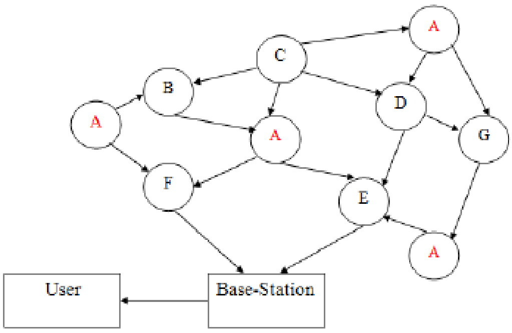

Fig. 1. Example of a Clone Node Attack [24]

A diagram of a wireless sensor network is presented in Fig. 1. In this figure, clone node A replicates on the network. Node A can communicate to neighboring nodes in the network. Clone knots cause various attacks within network.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Sachin Lalar*, Ph.D. Research Scholar, CSE, IKGPTU, Kapurthala, India. Email: sachin509@gmail.com
Shashi Bhushan, Professor, I.T., CGC, Landran, Punjab, India. Email: shashibhushan6@gmail.com
Surender, A.P., Computer Appl GTB, Bhawanigarh, India. Email: ssjangra20@rediffmail.com

*Retrieval Number: L3345081219/2019©BEIESP
DOI: 10.35940/ijitee.L3345.1081219
Journal Website: www.ijitee.org*

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

Clone node A can receive a valid packet from a legitimate node and discard the packet. Therefore, packet retransmission affects network performance. In Section 4 we will use the ns2 simulator to see the effects of the clone node in wsn. The next section describes the various attacks initiated by the clone node.

III. ATTACKS CAUSED BY CLONE NODE

This section examines the various attacks that may be launched by the clone nodes. These attacks are explained layer by layer of wireless sensor network. There are five layers i.e. Physical, Data Link Layer, Network, Transport & Application layer in wireless sensor network.

A. Physical Layer attack

Physical attacks at the WSN are initiated by blocking the radio channel. The clone node can send the wireless signals continuously on a wireless channel which will affect the other sensor nodes. It is difficult to prevent physical attacks in WSN due to no physical control on individual sensor nodes. Jamming and radio interference are two physical attacks that may be launched by clone nodes [5].

1. Jamming

Jamming attack is designed to interference the normal processes of network. The clone node can send wireless signals continuously on a wireless channel. The clone node sends the high power signals to block the wireless channel and to avert the neighbour sensor node from being communicated. Continuously jamming attack by clone node can result in denial of service attacks in physical layer. If the large number of clone nodes produces jamming attack, then the whole network may completely jammed [6].

2. Radio interference

The clone node produces interference in an irregular manner which will be effect the neighbour sensor nodes. The neighbour node may transmit the data when clone node produces the radio interference in the wireless channel. Due to radio interference, the sender signal may either destroy or alter [7].

B. Data Link Layer attack

The function of data link layer protocols is to make access of the shared wireless channels among node. The clone node can violate the predefined protocol in the link layer. For example, the clone node can cause a collision of packets by interrupting or intercepting, causing the sensor node to be exhausted from power by repeated retransmissions. The following attacks can possible by clone node in this layer as:

1. *Collisions Attack*

The clone node forwards the data at the same moment when another sensor transmitting its data, which causes the packet to collide. There will be a change in the data packet when packet will collide which resultant create discrepancy in checksum at the receiver end. The packet will be ignored as invalid. Collision attack reduces the speed of transmission of legitimate sensor [8].

2. Exhaustion Attack (Continuous Channel Access)

The clone node may target a sensor node by requesting data or sending irrelevant information through the channel. The clone node will continuously make the collision of packet of same sensor node which produces the exhaustion among the sender node. The exhaustion attacks will starve the different node in the network which is waiting to access the channel [9].

C. Network Layer attack

The WSN network layer finds routes of destination. The clone node can make various attacks which can completely disturb the routing information. The following attacks can be possible by clone node in this layer.

1. False Routing

The clone node can propagates erroneous routing information in the network. The clone node can use three different ways by which the incorrect routing information may spread in the network. First, clone node may override the sensor node through a large volume of erroneous routing information. Second, clone node may alter the update routing packet and routes it to the network which either transmit in the wrong route or poison in routing of the network. Third, the network node maintains a cache that contains the most recent route information required by on demand routing protocols. Like the poison the routing table, clone node can poison the node's cache [11].

2. Hello Flood Attack

For this attack, clone node uses the Hello packet which is used for making connection with their neighbours. When the sensor receives hello packets, it predicates that source node is in its radio range. The clone node sends the Hello packets to all the sensors of the network so that they will consider clone node belong to their neighbours. This results in a large number of nodes sending packets to this unrealistic neighbour [12].

3. Acknowledgement Spoofing Attack

Cloning nodes may forge the necessary recognition during routing. The clone node simply sends erroneous information with an acknowledgment about the dead or alive node.

4. Black Hole

The clone node forwards the shortest route request to all legitimate nodes of the network. By receiving the shortest route information to base station, the sensors forward the packets to the clone node. The cloning node receives the messages & it will not only redirect these messages but also drop these packets. This will reduce the performance of the network [13].

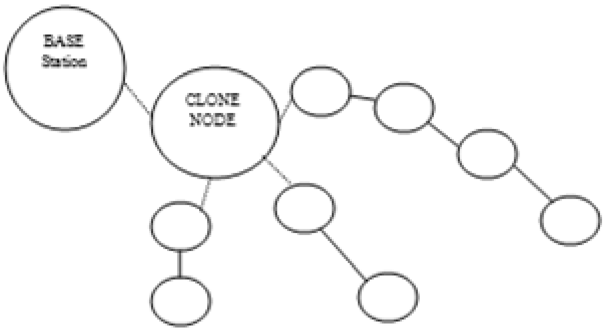

Fig. 2: Black Hole Attack by clone node

5. Sink Hole

The clone node is placed on a busy traffic route. The Clone nodes appear more attractive to surrounding nodes due to spoofing routing information. As a result, the surrounding node selects the clone node as the next node to transmit the data. Selective forwarding is very easy for this type of attack because entire traffic of network passes through the clone node [14].

6. Selective Forwarding

In this attack, the clone node may selectively drop the packets. The attack will be categorized in message selective & sensor selective forwarding. In the message selective, the cloning node simply sends the some selective information to the sensor node. In the second type, the clone node selects the nodes and discards the packets of the selected nodes.

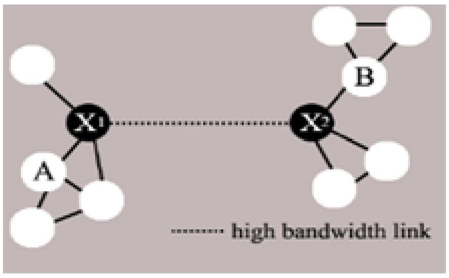

Fig. 3: Wormhole

7. Wormhole

This attack is possible if there are multiple clone nodes connected by high transmission channels or tunnels. That tunnel is assumed by other nodes as high transmission channel in the network. However, the packet transmission is selectively forwarded by the clone nodes. In Fig. 3, the clone nodes x1, x2 have a high bandwidth link between them and attract network traffic [15].

8. Packet Replication

The clone node continuously transmits the same packet in the network which will increase the network traffic.

D. Transport layer attack

In this layer, the clone node can launch the flooding, Energy drain, Injection false message & De-Synchronization attack which is explained below:

1. Flooding

The clone node can repeatedly make request for novel connection till the resources needed for connection are not depleted, or till it is not maximized. Flooding attack creates resource restriction problems for legitimate nodes.

2. Injecting false messages – data integrity attack

The main aim of this attack is to distort the sensor's information and negotiate the victim's exploration. The clone node injects the false message in the sender packet.

3. Energy drain attacks

As limited resources of sensor, the clone node can inject a fictitious report into the network or use the node to generate a large traffic in the network. The report could result in an erroneous alarm that wastes the node's response efforts and depletes the node's power. The focus of energy drains attack is to degrade the performance of the network.

4. De-synchronization

The clone node continuously sends the desynchronization request to other sensor nodes. The de-syn message disrupt of the existing connection among nodes. The clone node may send desynchronization messages to the node host causing retransmission of missed frames [17].

E. Application Layer Attack

The clone node can execute several types of attacks such as overwhelming, data aggregation attack in application layer.

1. Overwhelming

It is possible for the clone node to overwhelm a network node and the network will forward a large amount of traffic to the base station. This attack consumes network bandwidth and consumes the power of the node.

2. Data Aggregation Attack

The clone node can change in the data which have to aggregate and process to the base station. As a result, the base station mistakenly sees the environment being monitored by the sensor and can lead to improper behavior. When combined with black holes or sink hole with data aggregation, the data cannot reach to the sink station.

IV. SIMULATION AND RESULT

In this section, we will implement the clone node attack in the NS2 simulator. Eight different scenarios are used to investigate the influence of the clone node attack on the network. The first scenario uses a normal network to find the network performance in packet loss %. In the second scenario, the clone node is placed in the same network and checks the performance with same parameters. The first four scenarios, clone node initiates the black hole attack on the network. In last four scenario, the clone node produce the sinkhole attack in the network.

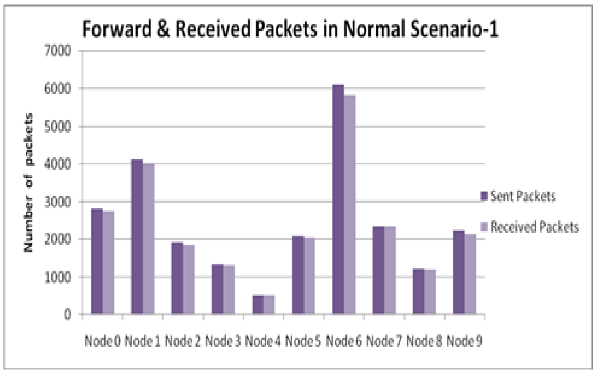

Fig. 4. Forward-Received Packet in Normal-Scenario-1.

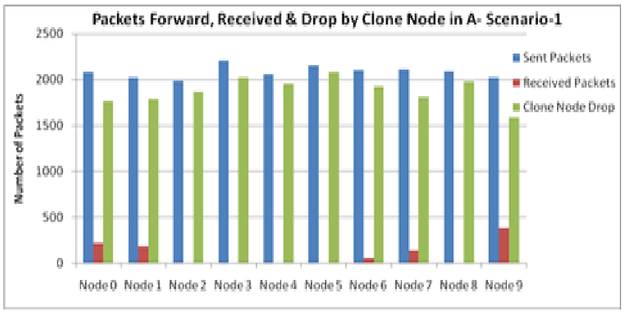

Fig. 5. Packets Forwarded, Received & Drop by Replication Node in Attack-Scenario-1.

We have compared the result in the packet loss parameter. To evaluate the performance, there are three figures for each scenario. The first figure shows the number of packets sent and received in the normal network without clone nodes. The second figure shows the forward, receive & drop packets in the containing cloned node network. The third figure displays the contrast of packet loss % in the network.

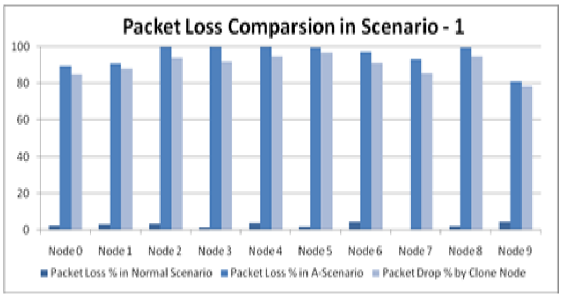

Fig. 6. Scenario-1 Comparison of Packet Loss.

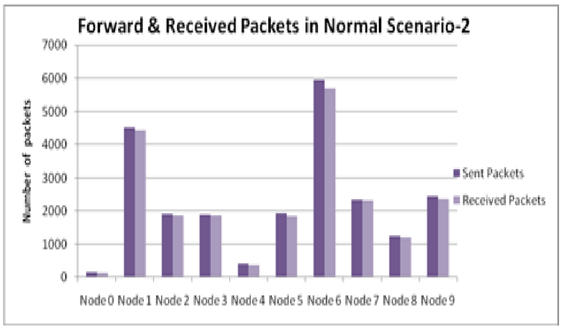

Fig. 7. Forward and Received Packet in Normal Scenario-2.

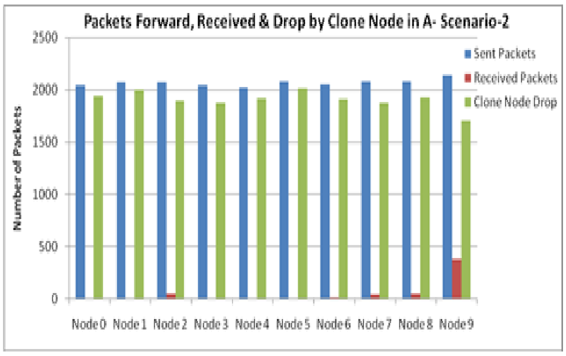

Fig. 8. Packets Forwarded, Received & Drop by Clone Node in Attack Scenario-2.

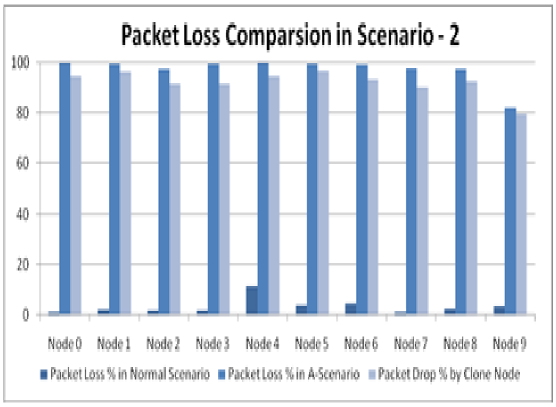

Fig. 9. Scenario-2 Comparison of Packet Loss.

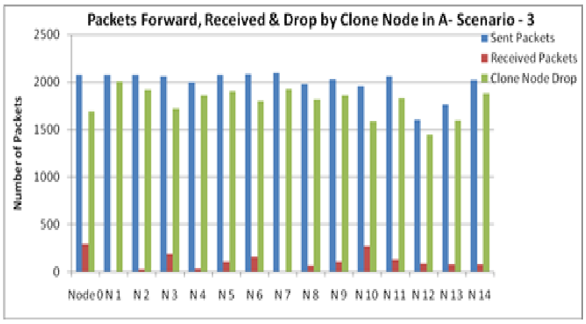

Fig. 10. Packets Forwarded, Received & Drop by Clone Node in Attack Scenario-3.

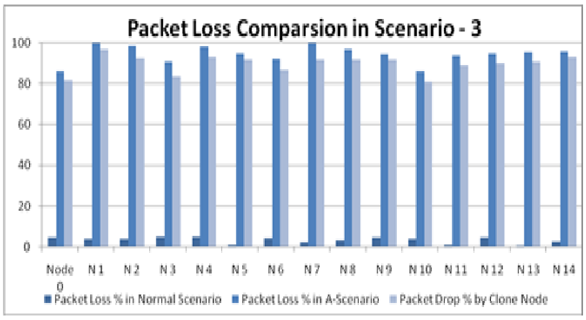

Fig. 11. Scenario-3 Comparison of Packet Loss.

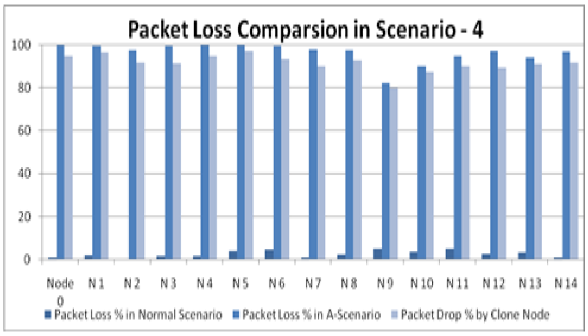

Fig. 12. Scenario-4 Comparison of Packet Loss.

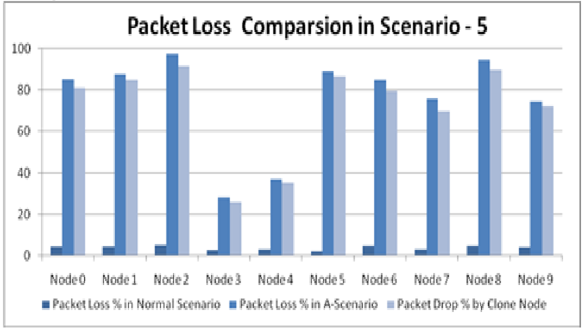

Fig. 13. Scenario-5 Comparison Packet Loss.

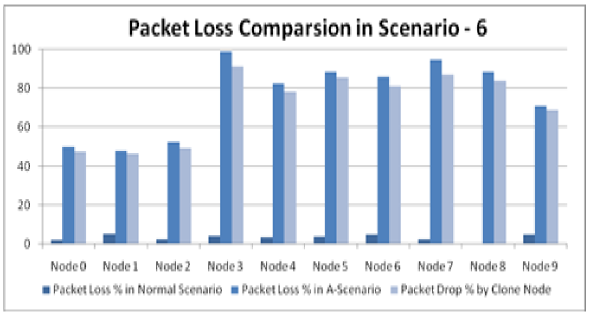

Fig. 14. Scenario-6 Comparison of Packet Loss.

Retrieval Number: L3345081219/2019©BEIESP
DOI: 10.35940/ijitee.L3345.1081219
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

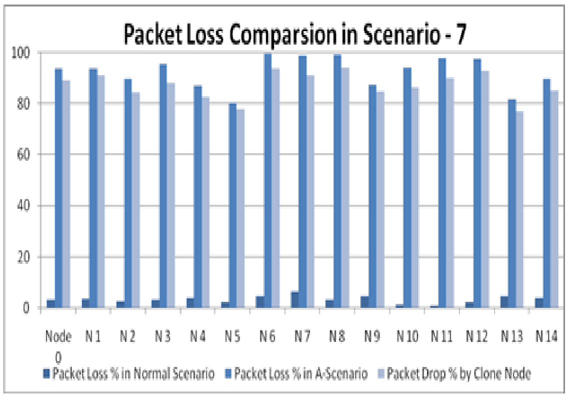

Fig. 15. Scenario-7 Comparison of Packet Loss.

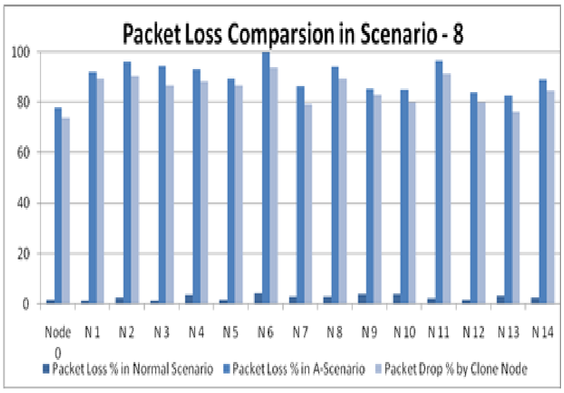

Fig. 16. Scenario-8 Comparison Packet Loss.

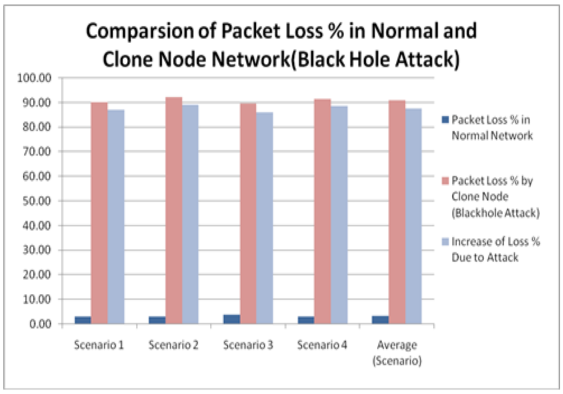

Fig. 17. Packet Loss % Comparison in Normal and Clone Node (as black hole) Network.

Analysis:

It has analyzed from the fig. 17 that the packet loss % in sensor network is increased by 87% when replicate node launch the black hole attack. In each scenario, the packet loss is high when replicate node is extant in the sensor network.

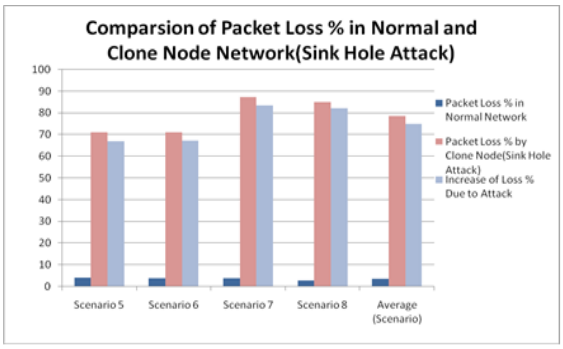

Fig. 18. packet Loss % Comparison in Normal and Clone Node (as Sinkhole) Network.

Analysis:

It has analyzed from the fig. 18 that the packet loss % in network is increased by 75% when replicate node launch the sinkhole attack. In each scenario, the packet loss is high when replicate node is extant in the wireless sensor network

V. CONCLUSION

Wireless sensor network is vulnerable to different type of threats. The paper examines the various attacks that can be caused by the clone nodes in the WSN. We also analyze the impact of replicate attack in the network. In first four scenarios, the clone node act as black hole, the average loss is increase by 87 %. In the last four scenarios, clone node act as the sink hole, the packet loss is increase to 75%. We have analyzed that network performance is degraded when the network has the clone nodes. In Future, we will try to find the new technique to prevention and identification of clone node in wireless sensor networks.

REFERENCES

1. Sachin Lalar, S Jangra, S Bhushan, "Study of Attacks & Countermeasures on Layers of Wireless Sensor Networks", International Journal of Control Theory and Applications, 10(15): 153-162.,2017
2. I. Akyildiz, S. Weilian,Y. Sankarasubramaniam & E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine*, *40*(8), pp 102-114, 2002.
3. H.C.Chaudhari and L.U. Kadam , "Wireless Sensor Network Security Attack and Challenges", International Journal of Networking, pp-04-16,2011.
4. D.Carman, P.S. Krus & B.J. Matt, "Constraints and Approaches for Distributed Sensor Network Security", *NAI Labs,Network Associates,2000.*
5. J.Deng, R. Han & S.Mishra, "Countermeasures Against Traffic Analysis in Wireless Sensor Networks", *University of Colorado at Boulder, 2004.*
6. M. Franklin, Z. Galil, andM. Yung, "Eavesdropping games: a graph-theoretic approach to privacy in distributed systems," *J. ACM*, vol. 47, no. 2, pp. 225–243, 2000.
7. X. Wenyuan, Ke Ma, W. Trappe, and Yanyong Zhang, "Jamming sensor networks: attack and defense strategies", IEEE 2006.
8. A. .D. Wood, J.A. Stankovic, and S.H. Son,"Jam: a jammed-area mapping service for sensor networks", Real-Time Systems Symposium, RTSS 2003. 24th IEEE, pages 286-297,2003.
9. Dr. Shahriar Mohammadi, Hossein Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensors Network" International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.3, No.1, pg 35-56, 2011.
10. D. .Sheela, K.Naveen and G Mahadevan, "A non cryptographic method of sink hole attack detection in wireless sensor networks", Recent Trends in Information Technology (ICRTIT), 2011.
11. Vinay Soni, Pratik Modi, Vishvash Chaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network" Volume 2, Issue 2, International Journal of Application or Innovation in Engineering & Management (IJAIEM)
12. Wazir Zada Khan Yang Xiang Mohammed Y Aalsalem, "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks", International Journal of Computer Network and Information Security (IJCNIS), 2011.
13. Devu Manikantan Shila, Tricha Anjali, "Defending Selective Forwarding Attacks in WMNs" Electro/Information Technology, 2008.
14. Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, Wang Liangmin, "Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks", pp.226-232, 2009.
15. Guorui Li, Xiangdong Liu, and Cuirong Wang, "A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks", pp.554-558, 2010.

16. Kashyap Patel , Mrs.T.Manoranjitham, 2013. “Detection of Wormhole Attack In Wireless Sensor Network”, India International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 5, 2013.
17. L. Hu and D. Evans, “Using directional antennas to prevent wormhole attacks”, *Network and Distributed System Security Symposium(NDSS)*, 2004.
18. Yih-Chun Hu, Adrian Perrig, David B. Johnson, “Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks”,INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE, pp. 267-279, 2003.
19. Virendra Pal Singh, Sweta Jain and Jyoti Singhai, “Hello Flood Attack and its Countermeasures in Wireless Sensor Networks”,IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11
20. Virendra Pal Singh , Aishwarya S. Anand Ukey , Sweta Jain, “Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks”, International Journal of Computer Applications (0975 – 8887) Volume 62– No.15
21. S.Madhavi and K. Duraiswamy, “Flooding Attack Aware Secure AODV”, Journal of Computer Science, 2013.
22. J. Douceur,“The Sybil Attack”, In Proc. Intl Wkshp on Peer-to-Peer Systems (IPTPS), 2002.
23.] M. J. Freedman and R. Morris Tarzan, “A peer-to-peer anonymizing network layer”, Proceedings of the 9th ACM conference on Computer and communications security, 2003.
24. Sachin Lalar, Shashi Bhushan & Surender,”An efficient tree-based clone detection scheme in wireless sensor network”, Journal of Information and Optimization Sciences, 40:5, 1003-1023, 2019.

AUTHORS PROFILE

Sachin Lalar is currently pursing Ph.D in the field of Wireless sensor network from IKGPTU, Kapurthala. He has been completed M.Tech from PEC Chandigarh. He has 10 years of teaching experience. He has published 12 research papers in various referred journals.

Dr. Shashi Bhushan has been working as Professor in the department of Information Technology, CGC Landran. He pursued his Ph.D from NIT Kurukshetra. He has more than 16 years of teaching experience. He had published more than 50 research papers in reputed journals and conferences including IEEE conferences.

Dr. Surender completed his M.Tech degree in Computer Science and Engineering from Ch. Devi Lal University Sirsa (Hry) in 2006, Ph.D in Computer Science and Application from Kurukshetra University, Kurukshetra in 2011.. He has more than 10 years teaching. Recently he is working as an Assistant Professor, in the Department of Computer Science, at GTB College, Bhawanigarh (Sangrur), Punjab, India. He has published over 50 publications in different International Journals and Conferences of repute.