International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

DETECTION AND PREVENTION OF SINK HOLE ATTACK IN AODV PROTOCOL FOR WIRELESS SENSOR NETWORK

Aayushi Bhatiya [1], Aditi Tilwankar [2], Dhawal Lambhate [3], Mr. Kakelli Anil Kumar [4]

1 B.E (CSE), (Roll No. 0818CS131005), Indore Institute of Science &Technology, Indore (M.P), India
2 B.E (CSE), (Roll No.818CS131015), Indore Institute of Science & Technology, Indore (M.P), India
3 B.E (CSE), (Roll No. 0818CS131049), Indore Institute of Science &Technology, Indore (M.P), India
4 Dean &Associate Professor, Department of CSE, Indore Institute of Science & Technology, Indore(M.P),India

---

Abstract - *Wireless Sensor Network is a collection of autonomous nodes connected to each other without any physical medium. Autonomous sensing nodes sense the target area, monitor the area, gather information and transfer it to the base station. As they are connected without any physical medium they are severe to many types of attacks. Sinkhole attack is an injurious active attack. Sink hole absorbs all the data transferred by the sender to the receiver by making itself a sinker/absorber and represents itself as the nearest neighbour by providing quick reply with high quality frequency to sender. Sink hole (network layer attack) is capable to launch other attacks on the network such as selective forwarding and wormhole attacks. It creates an enigma for the sender. ADOV routing protocol is used to send and receive data.Our paper tends to provide information on different type of WSN attacks, and mainly sink hole attack its detection and prevention.*

***Key Words*: WSN, Sink hole attack, AODV routing protocol, Throughput; Packet loss, PDR.**

1. INTRODUCTION

Wireless Sensor Network is the most recently using networks for the communication purpose in many areas. It is the area of research and development. WSN is a collection of nodes which are able to communicate without any physical medium. Their communication take place wirelessly by sending signals to each other.WSN sends packets to communicate. There is various applications of wireless sensor networks and they are broadly classified like environmental monitoring, acoustic detection, and seismic detection, military surveillance, inventory tracking, medical monitoring, smart space, etc. WSN faces many attacks and they are trouble for user and it is difficult to handle such attacks there are many different types of attack categorized on the basis of their impacts, data integrity, power consumption, routing, storage and so on they are Sybil attack, sink hole attack, black hole attack, flood attack etc.

Our main focus is on the routing based attacks in Wireless Sensor Network. Attacks based on routing don't follow routing protocols they modify such protocols to complete their task. An attacker in routing attacks overhears the exchange of information either it jams the signal of communication or it makes itself as the receiver.

WSN consist of motes, nodes, transceiver, gateway, application manager, and sink [2].All this together form a sensor node which is able to communicate and store i00nformation. Sensor node works on different layers [7].Application layer where node is present and allowed to communicate. Sensor nodes CPU is present in Network layer and the communication subsystem formed combining MAC layers, physical layer and network layer together [6].

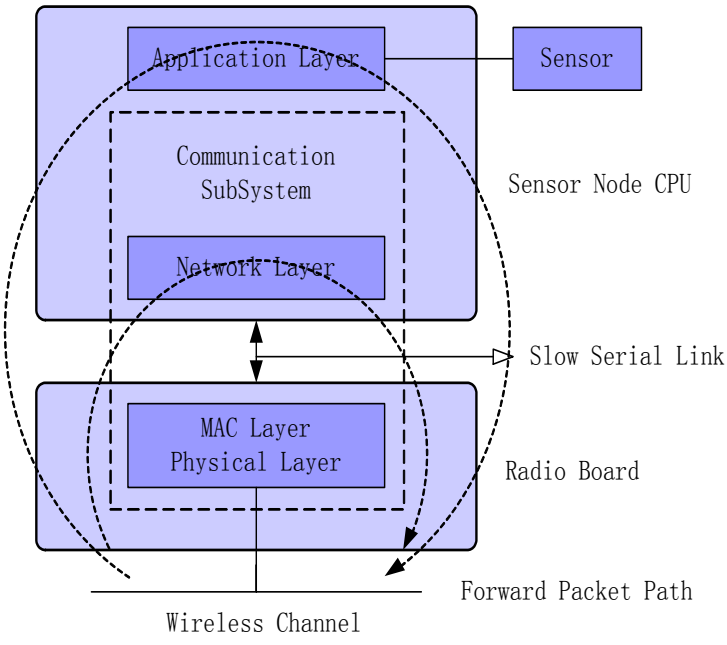

Figure 1: Overall architecture of sensor node and layers on which they communicate [1]

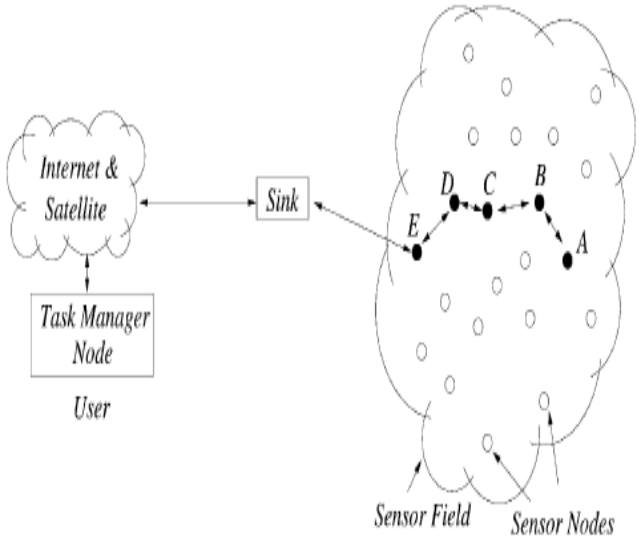

Figure 2: WSN communication architecture [2]

Characteristics of Wireless Sensor Network [1]:

1. Dynamic nature Scalability
2. Wide range of densities
3. Re-programmability Maintainability
4. Ability to face node failures
5. Mobility of nodes
6. Dynamic network topology
7. Heterogeneity of nodes

1.1 Security Issue

WSN is prone to different attacks which mean WSN is lacking some security issues. Security issue of WSN are mainly due to its no physical availability and the communication through signals. Some security issues with WSN are as follow:

1. Data integrity: Data integrity means the data transferred should be the same as it is send from the sender to the receiver there should be no modification in the data exchanged.The techniques like message digest and MAC are applied to maintain integrity of the data. Authentication of data should be maintained and which leads to data integrity.
2. Data Confidentiality: Data confidentiality means the data exchanged between two should be secure and no one else should know that any data is exchanged. It is a security protocol where sender and receiver are the only owner of information exchanged. Cryptography is techniques where data confidentiality can be achieved by encrypting data or converting it into cipher text.
3. Data Availability: Data availability means data should be available all the time to be exchanged between sender and receiver even if there is attack taking place.. Availability ensures that sensor nodes are active in the network to fulfill the functionality of the network.
4. Data Authentication: Data Authentication means data should be authenticate that the data transferred between the sender and receiver should not be modified during transfer. The data send through sender should be as it is as it reaches receiver. In asymmetric cryptographic communication digital signatures are used to check the authentication of any message or user while in symmetric key, MAC (Message Authentication Code) are used for authentication purpose.
5. Data Freshness: Data freshness means the data which is send earlier should not be repeated and the attacker can such data which is already sended. So, data should be fresh and new, freshness is achieved by using mechanisms like nonce or timestamp should add to each data packet.
6. Self-Organization: Every node should be independent and flexible enough to self organizing and self-healing itself according to the different situations.
7. Time Synchronization: Many WSN applications require group synchronization for tracking.
8. Secure Localization: Sensors get localized in the network as per their requirement to perform task due to some abnormal activities sensors get delocalized which makes communication improper.

1.2 WSN Attacks

WSN attacks are categorized on the basis of goal, performance, layer oriented, power consumption, routing and privacy attacks [5].

- **Goal oriented attacks:** Attacks based on the task they have to perform are called goal oriented attacks. These attacks can be active and can be passive.
  1. Passive attacks: Attacks which focuses to attack on data confidentiality. Passive attack encrypted traffic and capturing authentication information. Passive attacks don't allow the sender to acknowledge that the node to which it is communicating is not real. Some passive attacks are traffic monitoring, eavesdropping, traffic analysis attack all are type of passive attack.
  2. Active attacks: Attacks in which the malicious attacker is ready to attack and have knowledge of the nodes who is sender and receiver. DoS, modification of data, black hole, replay, sinkhole, spoofing, flooding, jamming, overwhelm, wormhole, fabrication, Hello flood, node subversion, lack of cooperation, modification, node subversion, man-in-middle attack, selective forwarding and false node all are the attacks which belong to the category of active attacks.

- **Performer-oriented attacks:** Attack which is of high capacity and performance who is able to harm the whole system by its effectiveness of attacking. They are of two type inside and outside attack.
  1. Inside performer –oriented attack: Attackers which are legitimate nodes of the native network and have access to the network information, and it is not easy to expect their attack patterns. Attack decreases the importance of information reaching the base station because of packet dropping at large scale. Several types of packet drop attacks are black hole, gray hole and on-off attacks.
  2. Outside performer-oriented attack: Attackers which are outside the network and control the transfer of data from outside. Denial of service, eavesdropping, resource exhaustion attacks are outside performer attacks where they deny the transmission.
- **Layer-oriented attack:** WSN nodes have different types of layers in them for communication purpose. This layered architecture makes these networks vulnerable to various kinds of attacks.
  1. Physical layer attack: Physical layer is more prone to attacks because of the lack of physical control over the individual nodes due to which jamming takes place. Jamming is the most dangerous attack at physical layer which interferes with the normal operations. It includes the layout of pins, voltages, cable specifications, hubs, repeaters, network adapters, host bus adapters and more[3].Attacks that occur at physical layer are eavesdropping, jamming, interception, radio interferences, tampering.
  2. Data link layer attack: Data link layer is the layer with functionality of connecting wireless channels with each other for communication and provide link abstraction to the upper layers [3]. Traffic analyzing, monitoring, disruption MAC 802.11, WEP weakness, channel exhaustion, unfairness, interrogation, Sybil attack are the attacks to which data link layer is prone.
  3. Network layer attack: Network layer is vulnerable to attack as if an attacker gets into it the whole network goes under his control. The Network Layer controls the operation of the subnet and how packets are routed from source to destination [3]. Attacker can spoof, alter, or replay routing information in order to disrupt traffic in the network. Attacks which take place here are black hole, sink hole, flooding, worm hole, node capturing, homing, locator disclosure, selective forwarding etc.
  4. Transport layer attack: Transport layer attackers ask for repeated connections which exhaust the node and attack takes place. Session hijacking, desynchronization, flooding etc are the attacks on transport layer.
  5. Application layer attack: Application layer is the layer from where the communication takesplace.TheApplicationLayercontainsavarietyofprotocolsthatarecommonlyneeded by users. NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, SMPP, SMTP, DHCP, SNMP, Telnet, Netconf[3].Different type of attacks can be carried out in this layer, such as overwhelm, repudiation, data corruption and malicious code. They consume bandwidth and energy nodes are drained out.

1.3 Routing protocol:

The nodes need protocol to communicate and form path for communication there are two types of routing protocols depending on the path and storage used by the node.

1. Proactive routing protocol: The routing protocol which carries the data all the time with it for communication. They are used for fixed node network area and maintain their own routing table.
2. Active routing protocol: The routing protocol which doesn't carries the data all the time with it and which is not limited to a specific networking area. They consume less bandwidth for communication.

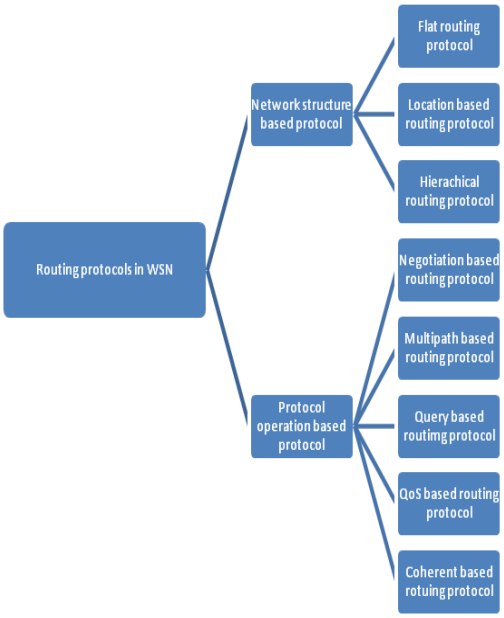

Figure 3: Types of routing protocol

Figure 4: Routing Protocols

- **Destination Sequenced Distance Vector Protocol (DSDV):** DSDV is a proactive routing protocol which maintains a routing table of every node and carries it all the time and use this table whenever data exchange is done between nodes. DSDV is a modification of conventional Bellman-Ford routing algorithm. It is used for exchange of data along with changing of arbitrary paths of interconnection which may not be close to any node. The information is broadcasted in two ways: full dump and incremental dump. DSDV maintains the shortest and best path for all the nodes by reducing the entries in the routing table. DSDV guarantees loop free path [9].Wastage of frequency bandwidth due to unnecessary advertising of routing information even if there is no change in the network topology. DSDV doesn't support Multi path Routing. It is difficult to determine time delay for advertisement of routes [8].
- **Ad hoc On Demand Routing Protocol (AODV):** AODV uses on demand approach for finding routes that means a route is established only when it is required by a source node for transmitting data packets. In AODV the source node floods the route request packet in the network when route is not available for desired destination. It may obtain multiple routes to different destinations from a single route request. AODV routing protocol is developed as an improvement to the Destination-Sequenced Distance-Vector (DSDV) routing algorithm. The aim of AODV is to reduce the number of broadcast messages sent throughout the network by discovering routes on the basis of demand of path the node wants to follow instead of keeping complete up-to-date route information [9]. Route request packet contains the IP address of the source node, sequence number, the IP address of the destination node, and the sequence number known of the last node of the system.
- **Dynamic Source Routing Protocol (DSR):** DSR protocol is an efficient and simple routing protocol developed specially for MANET. It is an on- demand routing protocol includes information in packet overheads. Every sender is able to control the multi–paths and choose a path through which it wants to send the data. The route maintenance does not locally repair a broken link and the connection establishment delay is higher than in table-driven protocols. It works well in low mobility environments and the performance of DSR decreases as mobility increase**s**.

2. AODV Routing Protocol

AODV Routing works by using Route Request Messages (RREQ) and Route Reply Messages (RREP).If a node is not in range with a node that it wants to talk to; it sends a RREQ to its neighbors. The RREQ contains source IP address and sequence number, and destination IP address and sequence number, as well as the life span of the RREQ.If a neighbor of the source doesn't know the route to the destination, it rebroadcasts the RREQ.

2.1 Sinkhole Attack in AODV

A node generates route request packet (RREQ packet) every time, it increase its sequence number by one and route request packet includes the sequence number. This sequence number is used to avoid multiple transmissions of the same RREQ. Higher the sequence number indicates fresh message. The malicious or attacker node overhears the communication channel as a part and observes the sequence number of all nodes. An attacker modifies the sequence no and source route in route request packet to launch the sinkhole attack. Attacker Node doesn't have unique id. An attacker node generates bogus route request packet by modifying the sequence no.

An attacker node carefully observe the sequence number of the target node and send the bogus route request packet whose source node is the target node with a higher sequence no. than the sequence no of the target node. Any node receiving this fake route request, see the higher sequence number and believe that it is the recent fresh route request. The node updates its cache, delete route from the target node and store the new fake route in the cache and will ignore all route request packets from the target node because the sequence number is less than the previous route request message. All the traffics are diverted to the sinkhole node.

2.2 How to find the Attacker Node?

- Attacker Node doesn't have a unique id or its id doesn't match the unique id of the source node.
- Frequency of attacking node and source node does not match.
- Each node maintains routing table so in routing table there will be another node i.e. attacker node..
- Sender node will identify its own neighbor.

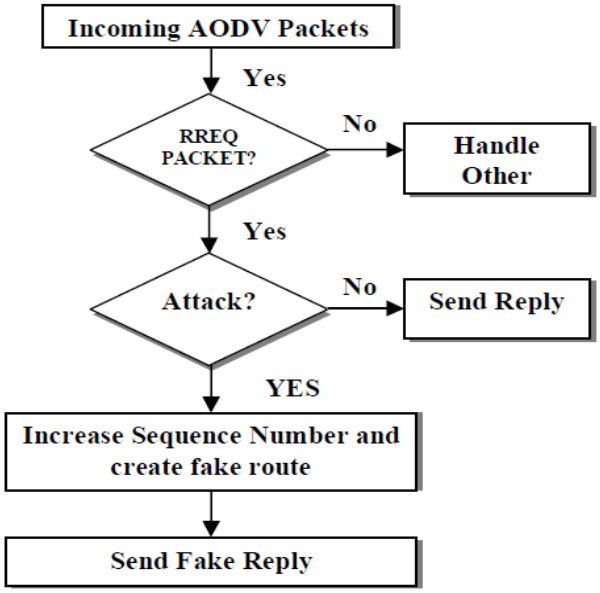

Figure 5: Framework for Sinkhole Attack

2.3 ANALYSIS OF SINKHOLE PROBLEM

Main aim of sinkhole node is to represent itself as the best and the nearest node in the system which is best suited for the sender node to send data which makes the sink node more attractive to other nodes and the traffic gets increased and every node starts rushing towards sink node which creates heavy traffic.

Sinkhole attacks are difficult to encounter because of the routing information supplied from one node to another node is difficult to verify. As an example, a wifi router adversary has a strong high-quality signal route through which transmitting of data is fast and it is accessible to those who have the features and presents themselves as eligible one for connection with wifi. The Wireless Sensor Network supports multiple communication patterns, where numbers of nodes send data at a time to one base station, this type of situation is favorable for sinkhole attacks. Sinkhole attack attacks only on the neighborhood node, not all the sensor nodes.

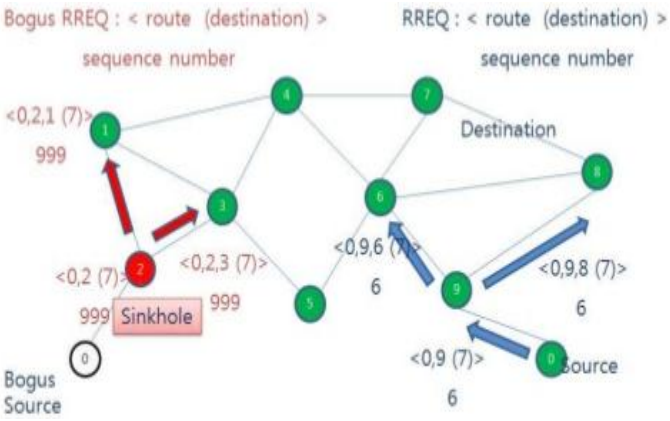

Figure 6: Production of Bogus RREQ

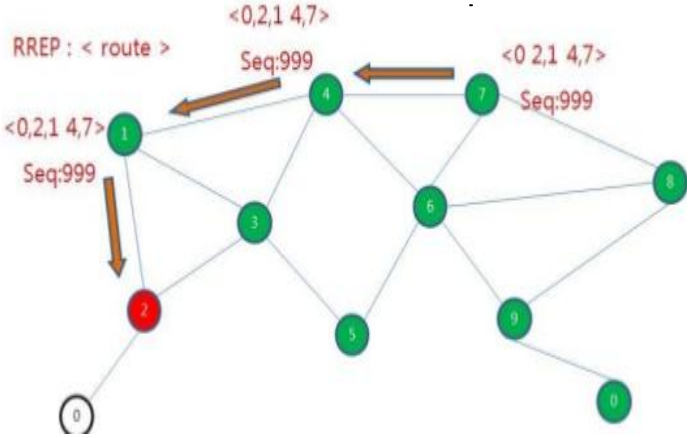

Figure 7: Bogus RREP generation

Sinkhole node attempts to draw all network traffic to itself. Afterwards it alters the data packet or drops the packet silently. Sinkhole attack increases network overhead, decreases network's lifetime by boosting energy consumption, finally destroy the network.

In the figure-7 the sequence number of the sink node is very high in comparison with the legitimate receiver node and the speed of sending RREP is very fast which makes the sender to think that it is the legitimate receiver with whom I want to share data as its being very near to me.

3. DETECTION OF SINKHOLE ATTACK

There are some different methods for the detection of Sinkhole Attack. The methods are as follows:-

3.1 Detection by IDS

First of all, we need to detect the malicious node. When we send the request packets from source node to destination node, then the malicious node do allow the request packet to reach the destination. Instead, it attacks the request packet and takes the request packet with it. Then it sends a fake routing acknowledgement to the source node.

For detecting the malicious node, we need to assign a unique sequence identity to each of the original nodes. All these

methodology comes under the Intrusion Detection System (IDS).

Sinkhole attack can also be detected by Routing Table and Frequency Detection but the most feasible method for this is IDS system.

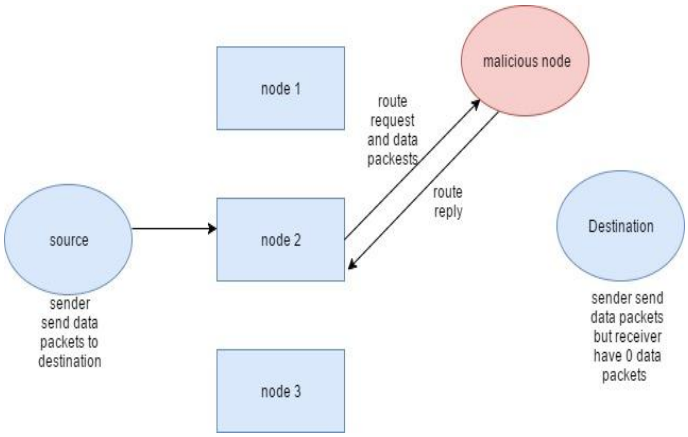

Figure 8: Attacker is receiving packets

In above diagram all data packets are received by attacker. So we find the malicious node and then prevent.

3.2 Detection by Route Monitoring Table

The detection is based on the timing information and destination sequence numbers that is maintained in the Neighborhood Route Monitoring Table. The table manages the time of Reply of the nodes from one to another and creates a record of it. A black hole node will send a route reply message to the sender without checking the details of the sender node as the legitimate node normally does by checking the routing table of the sender node. Reduction in reply time is used to detect the sinkhole node.

3.3 Anomaly-based detection

In anomaly based detection the normal user behavior is defined and intrusion detection is searching for anything that is anomalous in the network. Anomaly means different so the change in node in the system makes other nodes to detect the anomalous node present. Anomaly based detection approach includes the rule based and statistical approaches are also included under [10].

By the help of one system RSSI (Received Signal Strength Indicator) we detect the sink hole. RSSI value used EM (Extra Monitor) for detect the malicious node. High communication range of extra monitor node and their function to calculate RSSI of node. Sends the calculated data to base station with ID of source and next hop. Process initiates itself instantly when nodes are deployed the base station uses that RSSI value to calculate VGM (visual geographical map). VGM represents the position of each node present in the system later on when EM send updated RSSI value the base station identifies that there is some change in packet flow and as on comparison with the previous data it indicates that there is a sinkhole in the system. The compromised sink node is identified and isolated from the network by the sender (base station) using VGM value [10].

3.4 Statistical method

In statistical approaches the data associated with certain activities of the nodes in network is studied and recorded by researchers. For example monitor the transmission of packet between the nodes like CPU usage. The compromised sink node is detected after comparing the actual behavior of the nodes with the threshold value which is used as point of reference for the nodes and the nodes that exceed value of reference is considered as an intruder.

GRSh (Girshick Rubin Shyriaev) based algorithm proposed by Chen, et al for detection of malicious nodes in wireless sensor network. Base station calculates the difference of CPU usage for each node by monitoring them for a fixed time period. Base station identifies that whether a node is malicious or not on comparison of the difference of CPU usage with the threshold value.

Dynamic trust management system was proposed by Roy et al to detect and eliminate multiple attacks such as sinkhole attack. The calculation of trust by each node with its neighbor node based on experience of interaction between the two; recommendation and knowledge from the node is then sended to base station. The base station decided which node is sinkhole after it received several trust values from other nodes [10].

4. PREVENTION OF SINKHOLE ATTACK

Prevention of Sinkhole attack is mostly done by the IDS system.

INTRUSION DECTION SYSTEM

1) We provide a unique ID for each of the original nodes.

2) When the request packet is send by the source node, it identifies the unique ID of the destination node and the nodes through which the data packet is to be delivered.

3) The request data packets moves only through those nodes which posses unique identity.

4) When the request packet received by the destination and they give the acknowledgement or reply packet to sender then the data packets send by sender to the destination.

5) Data packet also have sequence number for security purpose.

6) And we send all data packets to receiver, all data packets are showing in result.

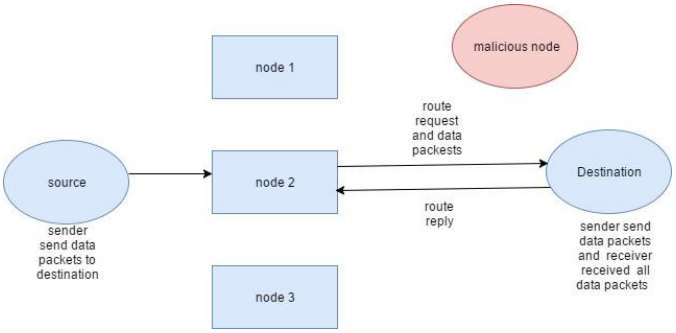

Figure 9: Authenticate receiver is receiving packets

In above diagram we can see that all data packets are received by receiver. And our data is secure form attackers.

5. Results

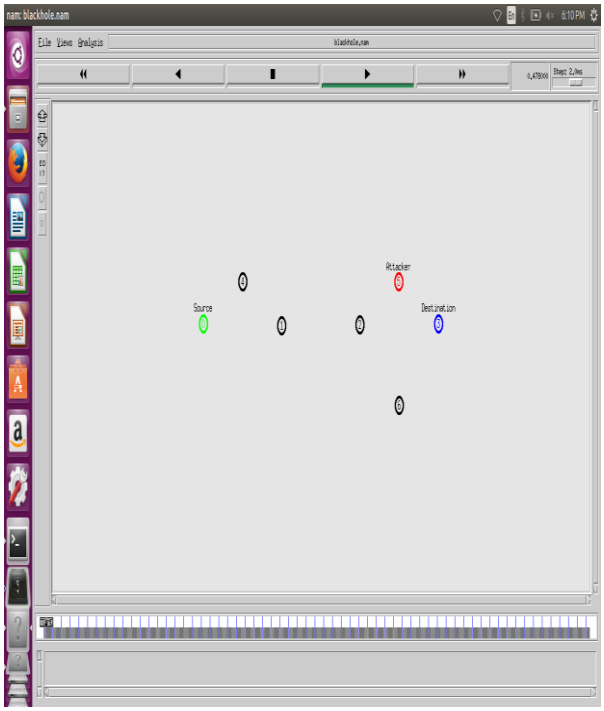

Figure 10: Nodes formation

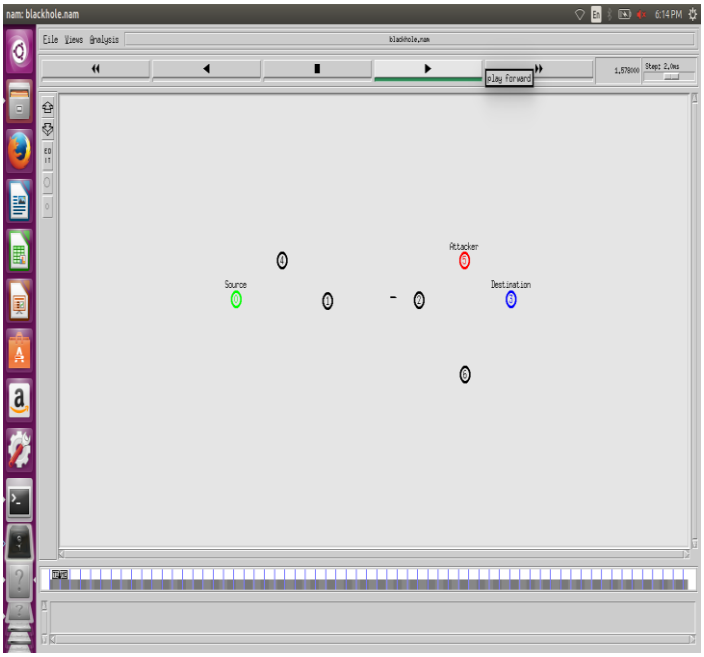

Figure 11: RREQ packet from sender to malicious node

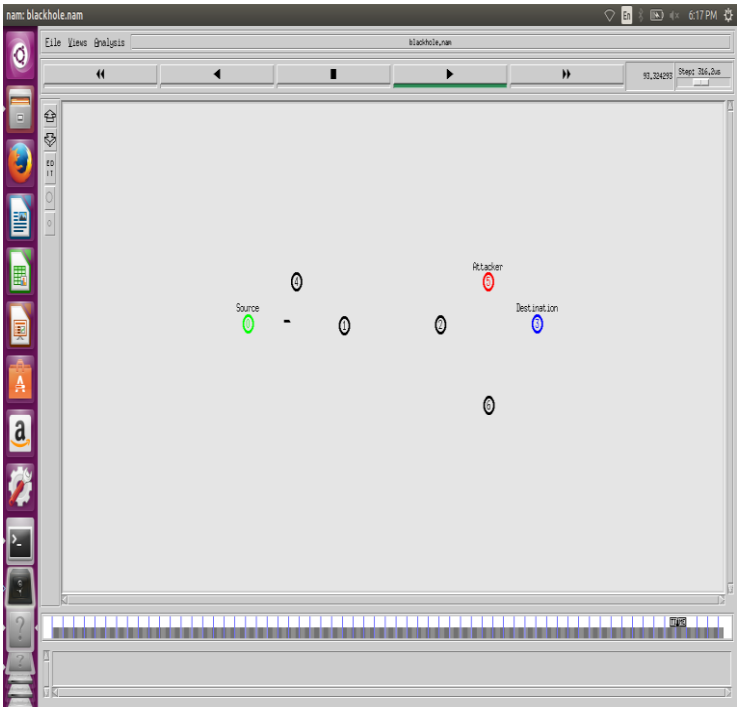

Figure 12: RREP from malicious node to sender

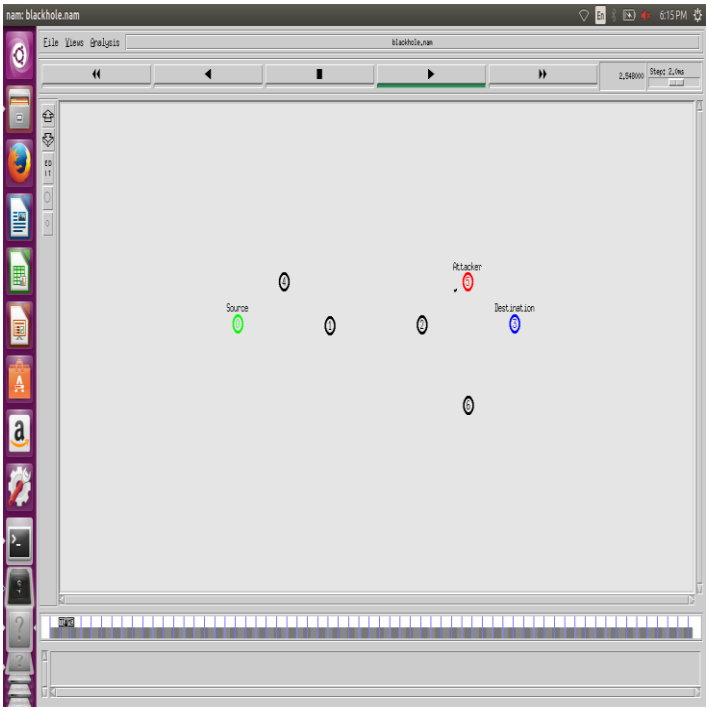

Figure 13: Data being sent to malicious node

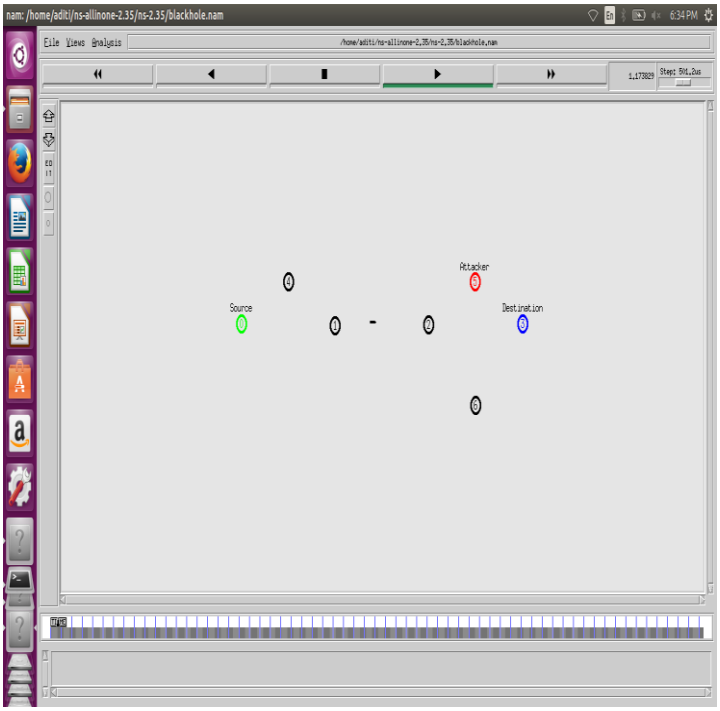

Figure 15: RREP from destination to sender with security mechanism

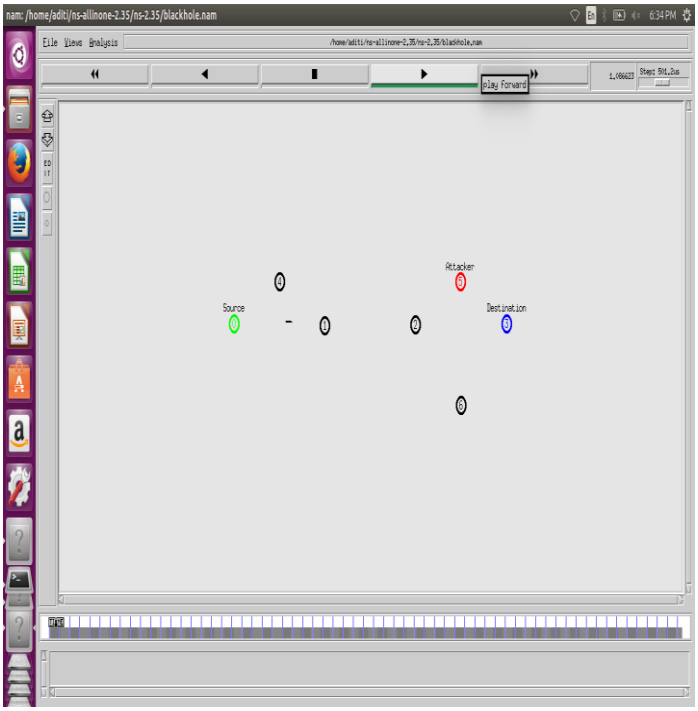

Figure 14: RREQ from to sender to destination node with security mechanism

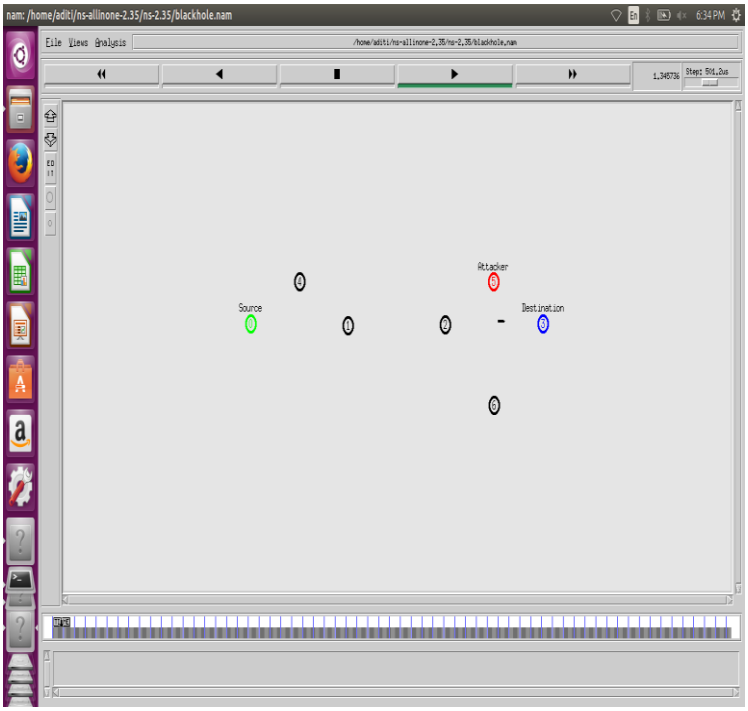

Figure 16: Data transferred to correct destination node with security mechanism

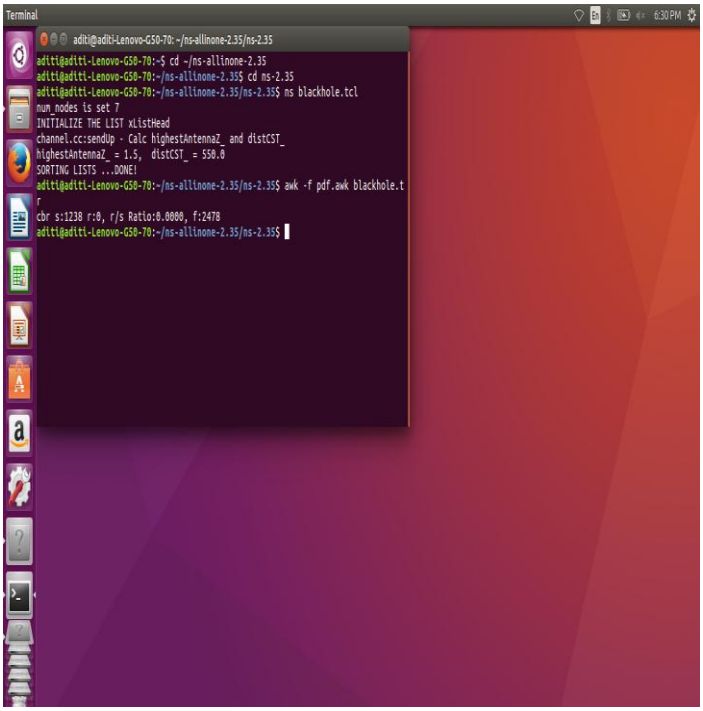

Figure 17: PDR is zero as no data is received by receiver

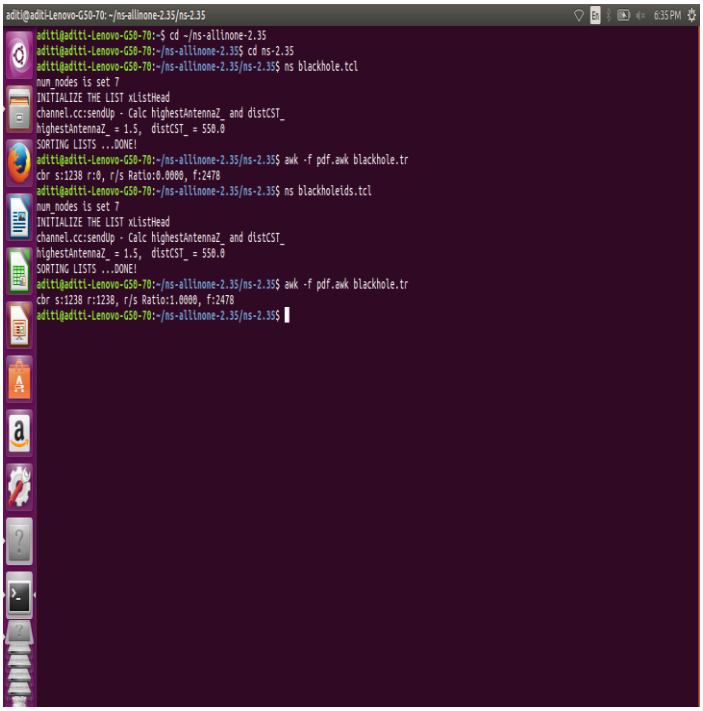

Figure 18: PDR is 1 as data is received by authenticate user

6. Conclusion

Wireless Sensor Network is a wide area of research where we all are concerned about the security of data transmission between the sender and receiver in a system .WSN are very much prone to the attacks that took place in the system .WSN are made much secure by using security algorithms and protocols. Mechanism of AODV protocol provides the security to the system for exchange of data and many more enhancements are there to be done in the system. NS2 is a simulation tool used by us in our work it provides simulation of the network and also functions as a tester. NS2 has OTCL and C++ in it as frontend and backend of the simulation tool to work on.

7. References

1. Wireless Sensor Networks WSN IEEE November 2005-v2 Krishna M. Sivalingam, Associate Professor Dept. of CSEE University of Maryland, Baltimore County (UMBC) Baltimore.
2. Wireless Sensor Network: A survey Arslan Munir EEL 6935.
3. Wireless Sensor Networks Wireless Sensor Networks Salvatore La Malfa.
4. Jaydip Sen. (2009). A Survey on Wireless Sensor Network Security, International Journal of Communication Networks& Information Security, 1(2).
5. Mohammed Ashfaq Hussain, Dr. A. Francis Saviour Devaraj, Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com, Vol. 3, Issue 2, March -April 2013, pp.1737-1741
6. Neelam Janak Kumar Patel, Dr. Khushboo Tripathi. Sinkhole Attack Detection and Prevention in WSN & Improving the Performance of AODV Protocol International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 5, May 2016
7. Guoyou He. Destination-sequenced distance vector (DSDV) protocol. Technical report, Helsinki University of Technology, Finland.
8. NisargGandhewar, Rahila Patel, "Detection & Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", 978-07695-4850-0/12 $26.00 © 2012 IEEE.
9. George W.and Camilius Sanga,"A Survey on Detection of Sinkhole Attack in Wireless Sensor Network"Kibirige Department of Informatics Sokoine University of Agriculture, SUA Morogoro, Tanzania georgekibirige

8.Biography

Aayushi Bhatiya is pursuing B.E (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. She is 4th year student. Her research interest are Artificial Intelligence includes and security mechanism in Wireless Sensor Network. She is continuing her research work in Artificial Intelligence and WSN.

Aditi Tilwankar is pursuing B.E. (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. She is 4th year student. Her Research interest is security mechanism in Wireless sens or network and Architecture of Wireless Sensor Network. She is continuing research work in security algorithms in WSN.

Dhawal Lambhate is pursuing B.E. (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. He is 4th year student. His research interest is Different Attacks on Wireless Sensor Network. He is continuing research work on Different attacks on Wireless Sensor Network.

Kakelli Anil Kumar is working as Dean in Dept. of CSE at Indore Institute of Science and Technology. He is having 14 Years of Teaching Experience at UG and PG engineering level. His Research interest includes protocols design and development in Wireless sensor network for quality Data Transmission. He is continuing research work in WSN, heterogeneous deployment and secures algorithms.

.