Detection of Packet Dropping Nodes in MANET using DSR Routing Protocol

Anshu Chauhan
M.Tech (IS)
Department of CSE
NIT Jalandhar, India

D.K. Gupta
Associate Professor
Department of CSE
NIT Jalandhar, India

Manoj Kumar Sah
Assistant Professor
Department of CSE
NIT Jalandhar, India

ABSTRACT
Wireless network is a growing technology that facilitates users for sharing of information instantly through wireless electronic devices irrespective of their locations. It can be infrastructure based or infrastructure less (ad hoc networks). An ad hoc network gains more attention because of its convenience, mobility, scalability, cost and easy setup. It is best suitable for applications, where predefined infrastructure is not possible. But ad hoc network is vulnerable to various attacks due to its functionality and deployment scenario. It is a decentralized networks therefore all the routing activities are handled by nodes. Nodes may behave badly in the network and can drop the packets instead of forwarding them. The aim of this research work is to detect these packet dropping nodes in MANET and prevents these packet droppers to be chosen as an active element of the path used for packet forwarding in DSR (Dynamic Source Routing) protocol. For this, we have implemented a trust and cluster based monitoring technique and simulated this environment using network simulator NS2.

Keywords
MANET; Vulnerable; Packet dropper; Wormhole; Man-in-middle attack; Spoofing.

1. INTRODUCTION
Mobile Ad-hoc network is an autonomous system of mobile nodes connected via multi-hop wireless links. It is a rapidly deployed network that can be formed and deformed quickly at anytime and anywhere without having any fixed predefine infrastructure. It is a self-organized network without having any centralized control. Therefore every node in MANET can perform the work of both host and router. Mobile Ad-hoc networks are also capable of handling topology changes. If a node leaves the network and causes link failure, still the network remains operational by network reconfiguration [3]. These properties make MANET quite efficient for applications like emergency services, rescue operations, military communication and Ad-hoc communication in urgent business meeting or lectures. Although it is a very flexible and popular technology still it is more prone to attacks as compare to wired networks due to its following limitations and security issues [4].

a) Mobile Ad-hoc network is highly dynamic in nature. In this, nodes can move anywhere in the network by which network can be disconnected frequently. Detection of attacks is quite difficult in this rapidly changing topology without having any central authority for trust management and monitoring purpose.

b) Providing security is a tedious task in MANETs because devices and information both are insecure for threats like spoofing and denial-of-service attack. We need some extra resources for configuring any security mechanism but resources are limited in mobile ad hoc networks.

c) In MANET nodes get energy from battery and this limited power supply can become the reason for their selfish behavior. In this, node uses the network resources for its own benefit and do not take active participation in packet forwarding.

The aim of this research is to detect these packet dropping nodes in mobile Ad-hoc networks. MANET supports frequent topology changes without having any central base station to configure. This makes routing, a challenging task in such a dynamic network. A variety of routing protocols has been proposed to find a path to be followed by data packets from source to destination. We can classify the MANETs routing protocols into following major categories.

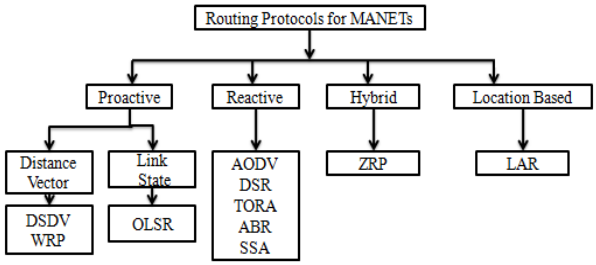

Fig 1 : Classification of routing protocols

Proactive routing protocols are also called table–driven routing protocols. They maintain an absolute picture of network at every single node in the form of tables. These are good for networks which have less node mobility or where nodes transmit data frequently. DSDV (destination sequenced distance-vector), WRP (wireless routing protocol), CGSR (cluster-head gateway switch routing protocol) and STAR (source-tree adaptive routing protocol) are some examples of table-driven routing protocols.

Reactive routing protocols are on-demand routing protocols. In which nodes do not contain complete information of the network topology, for the reason that it changes constantly. Path finding process and information exchange process execute when any node requires a path to communicate with the target node. Some examples of reactive routing protocols are: ABR (Associativity-Based Routing), AODV (Ad Hoc On-Demand Distance-Vector), LAR (Location-Aided Routing), DSR (Dynamic Source Routing) and TORA (Temporally Ordered Routing Algorithm). For our simulation we are using DSR routing protocol.

2. RELATED WORKS

Several defending mechanisms have been proposed to detect misbehaving nodes in MANETs. On the basis of their functionality we can classify them into following main categories: reputation based techniques, acknowledgement based techniques, and credit based techniques, game theory and intrusion detection systems [4].

2.1 Reputation Based Techniques

The phenomenon behind reputation based scheme is to degrade the reputation of misbehaving nodes by monitoring their behavior in the network. 'Watchdog' and 'pathrater' are used together to detect and avoid packet dropping nodes in MANET. They increase the network throughput in the presence of these malicious nodes in the network. 'Watchdog' is used to detect the malicious nodes and 'pathrater' is used to avoid these malicious nodes in the path, used for packet forwarding [1]. In 'watchdog' each node overhears the packet transmission by its neighbor node and detects the nodes; those are not forwarding the packets to other nodes. 'Pathrater' chooses the most reliable route for packet forwarding by collecting the information from each node about the misbehaving node. Some issues with this scheme are false reporting, huge detection time, collision and minor dropping. To overcome these issues, some extensions were proposed like 'Collaborative Watchdog' and 'CoCoWa' model. In collaborative watchdog, some sets of watchdog collectively take decision using Bayesian filters to reduce detection time and increase accuracy [9]. Hernandez-Orallo et. al., has proposed collaboration based 'CoCoWa' (collaborative contact-based watchdog) technique which is a combination of watchdog and sharing of information, when any diffusion takes place between two nodes. It reduces the time to give notification about packet dropping node [13].

2.2 Acknowledgement Based Techniques

In this, acknowledgement is sent by the node after receiving packets [5]. Kejun Liu el. at. has proposed the 2ACK scheme. In which, acknowledgement is sent by two-hops in the reverse path of packet and to reduce the overhead, only some packets are acknowledged.

2.3 Credit Based Techniques

The basic thought behind credit-based scheme is to encourage the nodes for providing faithful services to the network. To motivate the nodes for reliably performing network functions, some electronic benefits, rewards or currency system is set up. Each node gets some credit when it provides services to the network by forwarding the packets for others. And it uses same credit to pay other nodes for taking same services from them. Kurkure et. al. has proposed ARAN (Authentication Routing for Ad hoc Networks) based on this scheme [11].

2.4 Game Theory

Game theory is a multi-agent decision theory that can be used to study the distributed decisions made by decision makers to achieve some goals [6]. In ad hoc network game theory can be used to model conflict and cooperation among independent and rational decision makers. Nodes in ad hoc network have to make some decisions but they have limited information about other nodes in the network. Here game theory may help for monitoring other's action and make decisions. Each node in the network is a player of the game and will have their set of rules to be followed. Players can behave cooperatively or against one another. T.Evanjalin has proposed a technique based on trust model and 'stackelberg' game. In this game one player is head and rest had to follow rules otherwise they will be punished. Here game theory is use to broadcast the trust value of the nodes [12].

2.5 Intrusion Detection Systems

An IDS (Intrusion detection system) uses three models: signature-based, anomaly-based and specification based [7]. For MANETs specification based IDS is used rest two are designed for wired network. In specification based IDS some security specifications are maintained by the correct behavior of the node and when any incorrect behavior is noticed it is compared with the stored specifications and on the basis of the detection decision is made.

3. DESCRIPTION OF DSR

The dynamic source routing (DSR) is a reactive routing protocol, which is suitable for multi-hop mobile ad hoc network [2] [3]. This protocol restricts the bandwidth consumed by control packet by eliminating the periodic table update messages required in table-driven approach. In on-demand routing protocols every node uses some Becon (periodic Hello packets) to inform its neighbor of its presence. But DSR is Becon-less hence it does not require periodic Hello packets. The DSR works well in high rates of mobility and it has very rapid recovery mechanism, when routes in network changes. The protocol purely works on on-demad basis. It also allows the source node to choose multiple routes to destination for balancing the load. Its process contains two mechanism "Route discovery" and "Route maintenance". The fundamental method of route structure in DSR is to flood 'Route Request' packet in network. When destination node receives 'Route Request' packet it replies back to source by sending 'Route Reply' packet, which contains the route traversed by the 'Route Request' packet received.

In DSR, when a source node wants to communicate with some other node but no route is available for that particular node in its cache, it initiates 'Route discovery' mechanism. In this the source node broadcasts 'Route Request (RREQ)' packets to all its neighbors. Each node after receiving the 'RREQ' packet rebroadcasts it to its neighboring nodes further, if the node is not destination node or it has not forwarded it already. Each 'RREQ' packet contains sequence number generated by source node and the path it has traversed. Sequence numbers are important to ensure loop-free and up-to-dates routes. After receiving a 'RREQ' packet, node checks the sequence number before forwarding it. Packet will be forwarded only when it is not a duplicate packet.

In DSR, each node maintains a 'Route cache' that stores all possible information extracted from source route contained on data packets. This route cache is also used in 'Route discovery' process. If any intermediate node contains a fresh path to the destination in their route cache, then it replies by 'Route Reply' packet with entire route information to the source node. Node can also update its 'Route cache' learning from its neighbor route traversed by data packets if operated in the promiscuous mode. If route is not found by intermediate node then the destination node after receiving 'Route Reply' packet, replies back to the source node through the reverse path of 'Route Reply' packet has traversed.

In DSR, if any link has been failed or any node has changed its position then 'Route maintenance' mechanism is required. In this the failed route is removed first from the cache and if another route is not found in the cache for a particular node then again 'Route discovery' process is called.

Advantages of DSR Routing Protocol

a) Route is discovered only when it is required, it reduces the overhead of route maintenance.

b) Route caching reduces the cost of route discovery and intermediate node can also use the route cache information to reduce overhead.

Disadvantages of DSR Routing Protocol

a) Route maintenance mechanism does not repair broken links locally.

b) Stale route cache information may cause inconsistency and may pollute other nodes cache.

4. ATTACKS IN MANET ROUTING PROTOCOL

Currently MANETs are basically vulnerable to two different attacks: Active attack and Passive attack. Active attack is attack when misbehaving node has to bear some energy costs in order to perform the thread. In this the aim of malicious nodes is to damage other nodes by causing network outage. Active attacks can be internal or external. Internal attacks are injected by nodes within network while external attacks are injected by nodes outside the network. Passive attacks are performed mainly due to lack of cooperation with the purpose of saving energy selfishly. In this the aim of selfish nodes is to save their battery life for their own use. In this the attacks are classified as modification, impersonation, fabrication, lack of cooperation and DOS attacks [8].

4.1 Attacks Using Modification

In this type of attack the attacking node not only gain access but also may alter the fields of messages. For example a malicious node can launch DOS attack by modifying message fields or by forwarding routing message with false value, it may redirect the network traffic by setting false values in message fields.

4.2 Attacks Using Impersonation

Ad-hoc network is not currently being implemented by any kind of authentication mechanism as a result; malicious node can launch many attacks by impersonating any other node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network.

4.3 Attacks Using Fabrication

In this an authorized party inserts false information into the system. In MANET intruder generates false routing information and disturbs the network operation. Some fabrication attacks possible in MANET are as follows:

4.4 Attacks Using Fabrication

4.4.1 Wormhole Attack

This is also called tunneling attack. Wormhole attack is generally performed by the collaboration of two or more nodes connected via 'wormhole link'. This exploit gives the opportunity to attacker to short circuit the normal flow of routing packets by creating a virtual high speed network that is controlled by the two colluding attackers. Attacking nodes can selectively drop the packets and it may leak or modify the information by traffic analysis. They may also launch different attacks like man-in-the-middle, cipher breaking etc. In the figure 2 wormhole attack is set up by node 'A' and node 'I' with the help of a high frequency wormhole tunnel.

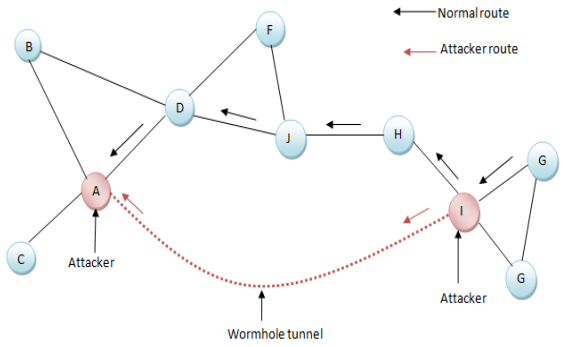

Fig 2 : Wormhole Attack

4.4.2 Blackhole Attack

In this attack a malicious node advertise itself as having a valid and minimum length to target. As in figure 3 node 'M' is a malicious node to launch blackhole attack in the network. When it receives a 'Route Request' packet, it immediately sends back a 'Route Reply' with a high sequence number to become an element of an active route. It has intention to consume or intercepts the packet without any forwarding. This can be launched by the cooperation of more malicious nodes and called cooperative blackhole attack which may cause more damage to the network.

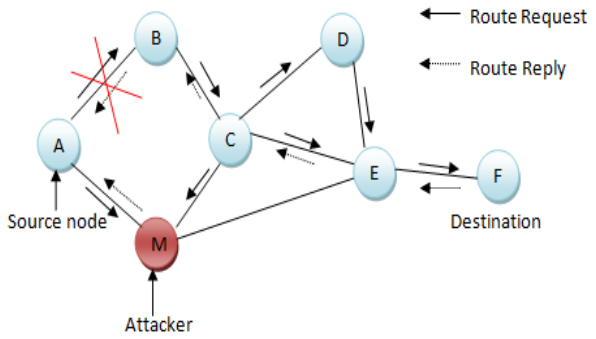

Fig 3 : Black hole Attack

4.4.3 Grayhole Attack

In grayhole attack malicious node shows uncertain behavior. Sometimes it may behave like normal node and may transfer every packet and sometimes it may drop some or all packets. It may also behave as malicious for some specific destination node and due to this nature it is hard to detect as compare to blackhole attack.

4.5 Attack due to Lack of Co-operation

Routing protocol in MANT assumes that all nodes in network are cooperative in nature but some nodes may use network for their own benefit and these nodes are called selfish nodes. These selfish nodes use the services of network but do not provide services like packet forwarding, to the network. Their aim is to save their resources like battery power, memory, bandwidth and CPU time.

5. PROPOSED WORK

In our proposal, we will use the monitoring of neighbor concept. But in our work every node will not be the monitoring node because in mobile ad hoc network every node has limited battery power so every node should not be in listening mode it will degrade its service time. Firstly we will create some overlapping clusters and each cluster will be having on monitoring node. These monitoring nodes will detect packet dropping nodes in their zone area and maintain

trust information about each node of their zone and will provide this information to the source node as well as other cluster's monitoring node when ever required.

5.1 Procedure

Whole process is divided into following three mechanisms**:**

a) Election of Monitoring Nodes

In this process some virtual overlapping clusters will be formed and in each such cluster there will be one monitoring node. Monitoring node will be selected on the basis of two factors i.e. node degree and power status. Node Degree will tell about the number of nodes in direct communication range of any node. And power status will be the measure of signal strength of a node. Node having highest node degree and power strength will be chosen as monitoring node. We will choose as many monitoring nodes so that every node should be in direct contact of at least one monitoring node. For a particular cluster this monitoring node will not be permanent after some time this process will be called again so that every node may get a fair chance to be chosen as monitoring node. Each monitoring node will maintain information about its neighboring nodes in the form of following table:

Node Address	Buffer	Trust counter	Trust Status

Table 1: Fields maintained by monitoring nodes

Node Address: This will be the network address of the neighboring nodes.

Buffer: Memory space to store last forwarded packet to that particular node by the monitoring node.

Trust Counter: This will indicate the current recorded behavior of node. Initially the status of neighbor nodes is initialized to zero.

Trust Status: Three values are possible for this field: Fair (F), Suspected (S), Packet dropper (D).

Threshold value: The value at which node is declared as malicious node in our simulation this value is set to 0.8.

b) Detection of Suspected Nodes

Each monitoring node overhears the node of its zone area and compares its sent packet from the corresponding stored packet in the buffer. If it matches the monitoring node release buffer for that node otherwise it increments the corresponding 'trust counter' field value by 0.2. For any node when this trust value reaches to threshold value it will be considered as suspected node and its 'trust status' field will be set as 'S'.

c) Process for Suspected Nodes

For a suspected node this process will be called. In this the monitoring node will send a fake RREQ with (TTL=1) message to the suspected node and will wait for the response of the suspected node. If the suspected node broadcast this RREQ message to its neighbors then its 'trust counter' will be decremented by 0.4. Otherwise it will be announced as packet dropper node and its 'trust status' will be set as 'D'. Monitoring node of one cluster will also share this information with its neighboring cluster's monitoring node. Whenever DSR will found any path to send data packets it will share this path with monitoring node of its zone. Monitoring node will verify the path by the information in its table. It will send a positive reply if no packet dropping node is present in the path chosen for data forwarding.

5.2 Proposed Algorithm

Assumptions:

M= total number of nodes,
N_i= particular node,
C_k = particular cluster,
Q= maximum nodes possible in the cluster,
P= packet,
B_i = buffer,
TC_i = trust counter (initially zero for every node),
TS_i = trust status (initially 'F' for every node) Th= 0.8

Algorithm

Step 1: Election of monitoring nodes

```
for ( i =1 to M)
{
  Calculate node degree ();
  Calculate power status ();
 }
while (every node is not in at least one cluster)
  {
   if (Ni = = max (node degree and power status))
            {
                Add   Ni into  Ci
             }
     if (number of nodes in cluster > Q)
            {
                k++;
            }
   }
```

Step 2: Detection of suspected nodes

```
while (TCi < Th)
{
   if (Ni   forwarded packet P to node Nj)
            {
              Bi [Top] = Bi [Top] + P;
               Bi [Top+1] = Bj [Top];
             }
   if (Bi [Top] = = Bi [Top +1] )
            {
            Bi [Top] = Bi [Top] - P
            }
   else
      TCi = TCi + 0.2 ;
     }
   if (TCi > = Th )
            {
            Set TSi as 'S';
            Go to step 3;
             }
```

Step 3: Process for suspected nodes

```
Send Test RREQ to the node with TTL=1
 if (response comes)
            {
              TCi = TCi - 0.4;
             }
 else
    Set TSi as 'D'.
```

Step 4: Call DSR ();

Step 5: Verify path by the information of monitoring node

6. SIMULATION RESULTS

Simulator is software that predicts the behavior of the computer network. Nowadays, many free and open-source network simulators are available that can simulate the MANTEs. Some notable network simulators are: NS (open source), OPNET (proprietary software) and NetSim (proprietary software). In our research work we are using NS-2.35 due to its best suitability for MANETs. Network Simulator (version 2) widely known as NS-2 is a discrete event-driven simulator targeted at networking research. It is suitable for both wired and wireless simulation of network functions, TCP, UDP, routing and multicast protocols [10]. It consists of two simulation tools: one is NS (network simulator) that contains all commonly used IP protocols and other in NAM (network animator) that is used to visualize the simulations. NS-2 has following features which makes it suitable for our project.

a. Environment set-up for ad hoc networks.
b. Wireless channel modules (e.g. 802.11).
c. Support of protocols like TCP, UPD and DSR.
d. Mobile hosts for ad hoc network.

6.1 Simulation Environment

The simulation of attack on DSR is deployed using ns-2.35 discrete-event simulator in mobile ad hoc network. Parameters are selected according to the requirement to get accuracy in results.

Parameter	Value
Simulator	Ns-2.35
Routing Protocol	DSR
Traffic Type	CBR(UDP)
Radio Propagation Model	Two Ray Ground
Network Area	1500 * 1500 m
Simulation Duration	50 sec
Number of Mobile nodes	15
Transmission Range	500 m
Max Queue Limit	50
Mac Type	Mac/802_11
Number if packet dropping nodes	2

Table 2: Simulation parameters

To correspond to the special distinctiveness and recital of network following metrics are used in our simulation:

Throughput: it basically measures the successful packet delivery over the entire simulation. It is calculated by dividing the total packets received by the total simulation time. Throughput may be affected by various factors like transmission medium, processing power of network components and end user behavior.

$$\text{Throughput} = Pr / (T_2 - T_1)$$

Where P_r is total data size received, T_1 is the start time and T_2 is the stop time of simulation.

Packet Delivery Ratio: PDR is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It basically measures the loss rate and characterizes both the correctness and efficiency of MANETs routing protocol. It represents the maximum throughput that the network can achieve. A high PDR is desired in a network.

$$PDR = (Pr / Ps) * 100$$

Where P_r is total packets received and P_s is the total packets sent.

Average end-to-end Delay: The packets end-to-end delay is the average time that packets have to pass through the network. This is the instance since the production of the packet by the sender up to its reception at the destination's application layer. It therefore includes all the delays in the network such as buffer queues, transmission time and delays included by routing activities and MAC control exchanges. It represents the reliability of routing protocols.

$$\text{Delay} = (T_2 - T_1)$$

Where T_2 is receive time and T_1 is sent time.

6.2 Different Scenarios

Figure 4 is showing the normal flow of DSR protocol in a mobile ad hoc network containing 15 nodes. Nodes are free to move in the network area and here node '0' is the source node and node '11' is the destination node. Attack is not injected in this scenario. In this case DSR has chosen the path (0-2-7-11) to forward packets up to destination node.

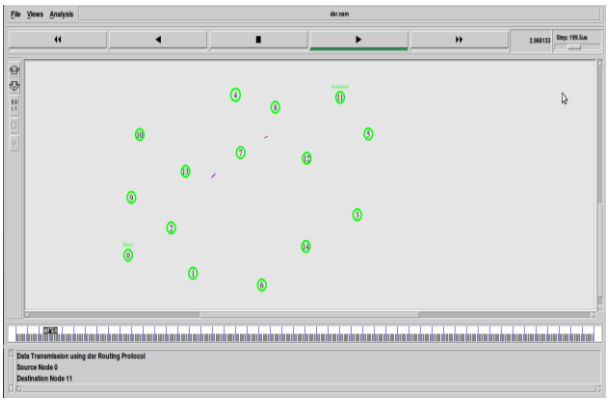

Fig 4 : Normal flow using DSR Routing Protocol

In the second scenario we have injected the packet dropping attack on node '7' and node '14' as shown in figure 5. In this case packets are dropped when they reach to the node 7 and most of the data packets are not reaching up to destination. Packet delivery ratio and throughput is decremented drastically in this case.

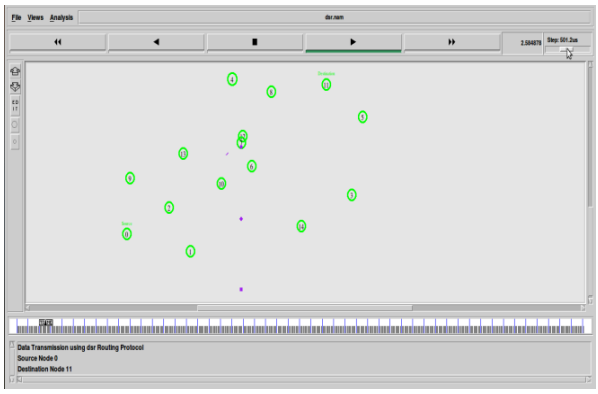

Fig 5 : Scenario containing Attack

In this third scenario we have applied the detection and prevention mechanism. Now DSR is following another route via (0-2-4-11) to send packets to the destination '11' as shown

in figure 6. It has avoided the path containing the packet dropper node.

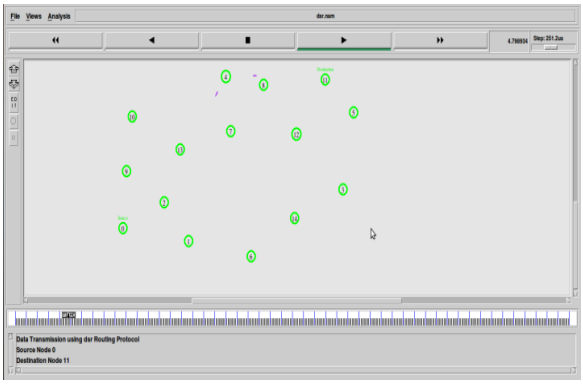

Fig 6 : Scenario After Prevention Mechanism

```
nespl@ubuntu: ~/Desktop/final project/15-nodes
  Details of source node are 2002, 1009
  Details of destination node are 6, 2005

  node 7 is behaving as packet dropper node
  node 14 is behaving as packet dropper node

nespl@ubuntu:~/Desktop/final project/15-nodes$ gawk -f pdr.awk prevention.tr

  Packet Delivery Ratio =  100.0000

nespl@ubuntu:~/Desktop/final project/15-nodes$ gawk -f parameters.awk prevention.tr

  Total sent packets = 1000
  Total received packets = 1000
  Average e-e delay(ms)= 17.25
  No. of dropped data (packets) = 0

nespl@ubuntu:~/Desktop/final project/15-nodes$ gawk -f throughput.awk prevention.tr

  Average Throughput[kbps] = 40.91
  StartTime = 0.00
  StopTime = 49.96

nespl@ubuntu:~/Desktop/final project/15-nodes$
```

Fig 7 : Detection of Packet Dropper Node and Parameters After Prevention

Figure 7 showing the results after detection and prevention process. It has been detected that node '7' and '11' are packet droppers. And after prevention mechanism packet delivery ratios has become 100 percent, which has been converted into 27.318 percent in case of attack on node '7' and node '14'. Figure 8 is representing the throughput graph between normal flow of DSR, flow when node '7' and node '14' is packet dropper and after prevention mechanism.

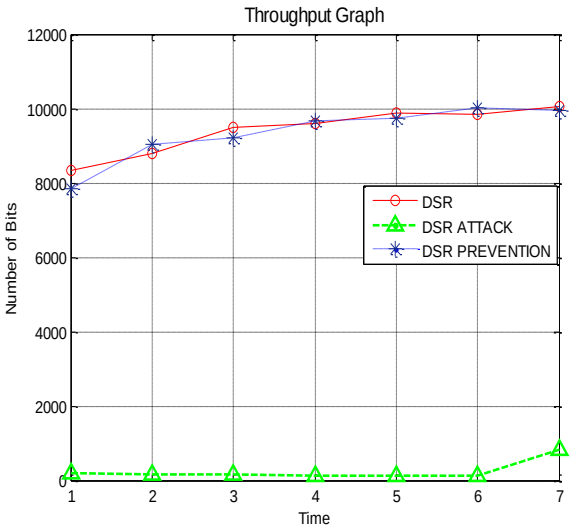

Fig 8 : Throughput Graph between Normal Flow, Attack and After Prevention

It is clear from figure 8, that packet dropping attack has put drastic effect on packet delivery ratio and throughput of the mobile ad hoc network. Throughput is decremented by 50 percent and packet delivery ratio is decremented by 70 percent by this attack. So packet dropping nodes are serious problem for network performance.

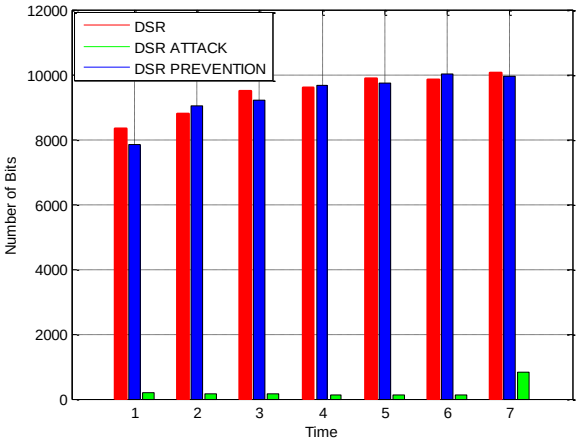

Fig 9 : Comparisons of Throughput Graph between Normal Flow, Attack and After Prevention

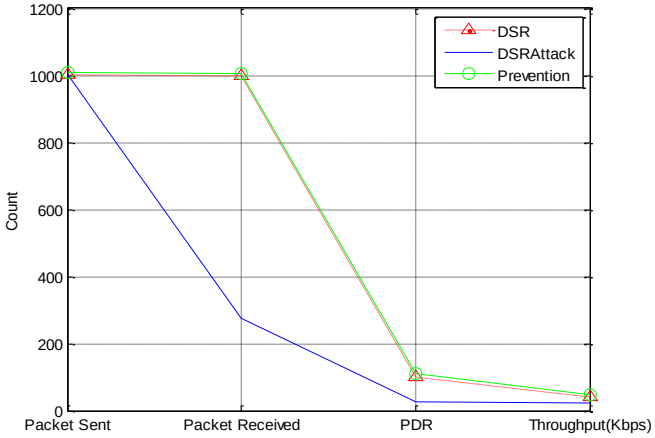

Fig 10 : Comparison of different Parameters in three cases for 15 Nodes

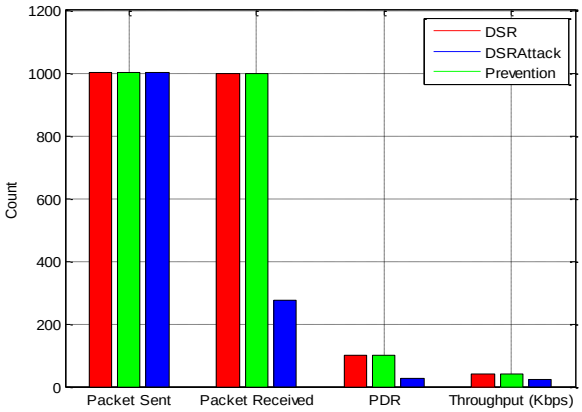

Fig 11 : Comparison of different Parameters in three cases for 15 Nodes

7. CONCLUSIONS

Security is always an open area of research and improvement. The configuration of security mechanism in ad hoc network is a challenging task due to its dynamic nature and resources constrains. This paper studies the effect of packet droppers on the flow of DSR routing protocol. The analysis shows that these misbehaving nodes have drastically degraded the network performance. In this paper a trust and monitoring based security mechanism has been implemented to detect and prevent these packets droppers. This mechanism divides the whole network onto some small virtual zones and for each zone only one monitoring node is being selected to detect the packet droppers. So some advantages with this mechanism are: its false detection rate is low and overhead on the network is also less. Simulation shows that a better packet delivery ratio and throughput has been gained again after prevention mechanism. Thus we have successfully injected, detected and also avoided packet dropping nodes from the path of DSR.

The ad hoc networking is an open challenging area of research in computer science due to its dynamic nature. This means ad hoc network contains lots of vulnerabilities to be explored and many other issues to be solved. In this thesis we have only focused to detect packet dropping attack on DSR routing protocol. In future our plan is to study some other vulnerable areas of mobile and hoc network. We will also try to configure this proposed mechanism with other routing protocols of MANET.

8. REFERENCES

[1] Sergio Marti, T. J. Giuli, Kevin Lai, Mary Baker, "Mitigation routing misbehavior in mobile ad hoc networks", ACM, proceedings of 6th annual international conference on Mobile computing and Networking, pages: 255-265, (2000).

[2] David B. Johnson, David A. Maltz, Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Carnegie Mellon University, Pittsburgh, (2001).

[3] Prasant Mohapatra, Srikanth V. Krishnamurthy, "AD HOC NETWORKS: Technologies and Protocols", Springer Science and Business Media, USA, (2005).

[4] Sevil Sen, John A. Clark, Juan E. Tapiador, "Security Threads in Mobile Ad Hoc Networks", University of York, U.K, (2010).

[5] Kejun Liu, Jing Deng, P. K. Varshney, K. Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transaction on Mobile Computing, Vol: 6, Issue: 5, (2007).

[6] Feng Li, Yinying Yang, Jie Wu, "Attack and Flee: Game-Theory-Based Analysis on Interactions among Nodes in MANETs", IEEE Transactions on Systems, Man and Cybernetics, Vol: 40, No: 3, (2010).

[7] Ahmed M. Abdalla, Imane A. Saroit, Amira Kotb, Ali H. Afsari, "Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol", Science Direct: World Conference on Information Technology, pages: 115-121, (2011).

[8] Praveen Joshi, "Security issues in routing protocols in MANETs at network layer", Science Direct: World Conference on Information Technology, pages: 954-960, (2011).

[9] E. Hernandez-Orallo, M. D. Serrat, J. C. Cano, C.T. Calafate, P. Manzoni, "Improving Selfish node detection in MANETs Using a Collaborative Watchdog", IEEE Communication Letters, Vol: 16, Issue: 5, (2012).

[10] Terrawat Issariyakul, Ekram Hossain, "Introduction to Network Simulation NS2" Second Edition Springer Science and Business Media, USA, (2012).

[11] A. M. Kurkure, B. Chaudhari, "Analysing Credit based ARAN to detect selfish node in MANET". IEEE International Conference on Advances in Engineering and Technology Research (ICAETR), (2014).

[12] T. Evanjalin, "Detection of Selfish Users and Prevent Using Game Theory in CRAHNs", International Conference on Simulations in Computing Nexus (ICSCN), Coimbatore, (2014).

[13] Enrique Hernandez-Orallo, Manuel D. Serrat, Juaun-Cano, Carlos T. Calafate, Pietro Manzoni, "CoCoWa: A Collaborative Contact-based Watchdog for Detecting Selfish Nodes", IEEE Transactions on Mobile Computing, Vol: 14, Issue: 6, (2015).