Analysis of DDoS Attack Effect and Protection Scheme in Wireless Mobile Ad-hoc Network

Ramratan Ahirwal

Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha (MP) 464001India
Ram2004_ahirwal2004@rediffmail.com

Leeladhar Mahour

Computer Science & Engineering
Samrat Ashok Technological Institute
Vidisha (MP) 464001India
laxmanmits@yahoo.com

Abstract

In Wireless mobile Ad Hoc Networks (MANET) every node functions as transmitter, router and data sink is network without infrastructure. Detecting malicious nodes in an open ad-hoc network in which participating nodes have no previous security associations presents a number of challenges not faced by traditional wired networks. Traffic monitoring in wired networks is usually performed at switches, routers and gateways, but an ad-hoc network does not have these types of network elements where the Intrusion Detection System (IDS) can collect and analyse audit data for the entire network. A number of neighbour-monitoring, trust-building, and cluster-based voting schemes have been proposed in the research to enable the detection and reporting of malicious activity in ad-hoc networks. The resources consumed by ad-hoc network member nodes to monitor, detect, report, and diagnose malicious activity, however, may be greater than simply rerouting packets through a different available path. In this paper we are trying to protect our network from distributed denial of service attack (DDOS), In this paper we present method for determining intrusion or misbehave in MANET using intrusion detection system and protect the network from distributed denial of service (DDOS) and analysis the result on the bases of actual TCP flow monitoring, routing load ,packet delivery ratio and average end-to-end delay in normal , DDOS attack and IDS time .

Keywords: **DDoS ,Ftp, Intrusion detection, Mobile ad-hoc network, Tcp.**

1.Introduction

In MANETs, nodes act as both routers and ordinary nodes. Due to dynamic network topology and lack of centralized infrastructure, network security has brought a new challenge to networking communities. Unlike traditional networks, MANETs are more vulnerable to DDoS attacks due to limited resources that force nodes to be greedy in resource utilization. When there is no cooperation, activities of even a small number of nodes may significantly decrease the performance of the network. MANETs are vulnerable to Distributed Denial of Service (DDoS) due to their salient characteristics. There is a need to provide an incentive mechanism that can provide cooperation among nodes in the network and improve overall network performance by reducing DoS attacks.MANETs have come into prominence due to potentially rapid infrastructure-less deployment in military and emergency situations. However, the unreliability of wireless links between nodes, possibility of mobile nodes being captured or compromised, break down of cooperative algorithms, all lead to increased vulnerability [10]. Unrelenting attackers will eventually infiltrate any system. It is important to monitor what is taking place in a system and look for intrusions. Intrusion Detection Systems (IDS) do precisely that. An IDS forms the second wall of defence in a high-survivability network. Intrusion prevention measures such as authentication and encryption are not guaranteed to work all the time, which brings out the need to complement them with efficient intrusion detection and response. If an intrusion is detected quickly enough, the intruder can be ejected before any damage is done or any data is compromised. Effective IDS can not only serve as a prevention to prevent intrusions but also provide information about intrusions to strengthen intrusion prevention measures.

The paper is organized as follows: Section 1 Provides Introduction , Section 2 provides some background work on IDS, Section 3 provides the problem statement, section 4 proposed scheme description. Section 5 provide threshold algorithm, section 6 Simulation parameter, 7 gives Simulation detail, Section 8 experimental result and 9 gives Conclusion, Section 10 Future work.

2. Previous Related Work

Recently proposed incentive mechanisms for enforcing cooperation among nodes can be classified into trade-based and trust-based mechanisms. Trade-based mechanisms assume market models for providing virtual currency incentives for motivating cooperation among nodes. In the trust-based models, trust is created and the service provider is stimulated by these trust values. Each scheme can be deployed in different application scenarios. The trade-based models are not applicable in cooperative networks where no financial incentives are needed to run the network. However, trust-based schemes can still be used to improve network performance.

In the trade-model proposed in [1], every device has a tamper resistant security module, PKI to ensure authentication. This security module is used for account management. Two billing models that charge nodes as a function of number of hops messages have travelled were proposed. An ad hoc participation economy (APE) that uses a dedicated banker node to manage accounts was proposed in [2]. Unlike the tamper-resistant mechanism, the APE uses dedicated banker nodes for account management and also has facilities for converting virtual currency into real monetary units. Incentive mechanisms that use a node as a transaction manager are not plausible in dynamic ad hoc networks since location tracking incurs additional overhead. A similar reputation-based mechanism known as a reputation participatory guarantee (RPG) was proposed [3]. This mechanism provides a network layer solution that detects selfish nodes without propagating reputation ratings in the network.

A trade-based model that relies on the accessibility of banker nodes was proposed in [4]. This model does not use any tamer resistant hardware but instead uses credit-clearance services in a wireless overlay network. In [5], a reputation-based model that investigates the effect of misbehaviour on network performance was presented. It uses a watchdog for identifying misbehaving nodes and a pathrater for selecting routes that do not select misbehaving nodes. In [6], CONFIDANT, a reputation-based model that removes misbehaving nodes by propagating bad reputation through the network was proposed. In [7], a reputation based model that only propagates positive reputations among the nodes was proposed. Reputation computation involves the aggregation of three different types of information based on different levels of observations and services. This method of reputation computation incurs greater overhead than other proposed schemes.

3. Problem Statement

Our aim is to protect our network from denial of service attack (DDOS), so MANET would require a security strategy to defend against existing and potential DDoS attacks. Because the MANETs the nodes may be individually controlled. It is difficult to apply a network wide security upgrade. Though an about to be deployed MANET can apply an updated defence strategy, any unpredictable, unforeseen DDoS attack technique in the future can threaten the network and put it in the same situation of those operating unsafe MANETs. A proper solution should require little or no change of the existing network system. It should not require a large-scale upgrade. It should not depend on cooperation from the individuals. It should be backward compatible and transparent to the other components of the network.

4. Proposed Scheme

We propose a new defence mechanism which consists of a flow monitoring table (FMT) of all the mobile node. It contains time, sender_id, node coordinate axis and receiver_id id, transport_info, protocol_type, event_type, event_time ,application layer_info in our approach we describe each module one by one .

We describe each value here time means actual simulation time , sender id contain sender node id, coordinate value contain actual position of the node at particular time, receiver_id contain at particular time receiving node number, transport_info hold TCP and UDP packet information at particular time, Protocol filed hold the value which type of protocol use like AODV, event_type contain (s,r,d,f) data send ,receives , drop and forward at the time. application layer_info contain FTP and CBR packet type. According to above parameter we analyse the bahiover of the network in normal case , DDOS attack case and IDS case.

4.1Normal Profile Creation

Here we uses NS-2 simulator for creation of mobile node and set all parameter to configure our network like radio range , application layer protocol , transport layer mechanism , routing protocol and data link layer protocol as 802.11 and also set physical layer information by using the NS-2 Simulator. After that we create sender and receiver nodes and send data packet through intermediate nodes because mobile ad-hoc network is temporary network and infrastructure less so that frequently change the network topology here we capture the information till the stop time of our simulation for further analysis.

Algorithm for Creating Normal profile using AODV routing protocol

Step1: Set start time , stop time;
Step2: set application data (FTP , CBR)
Step3: set transport layer agent (TCP , UDP)
Step4: Compute route through AODV with radio range 250 meter

```
If (next node r_range<= 250)
        {
                RREQ to next node until destination node;
        }
Else    {
                Out of range or destination not reach;
        }
```

Step5: Set MAC layer parameter (channel type , anntena type , prop mode)
Step6: Capture info (event, time,send_id , Rx_id , protocol type,transport_info);

4.2. Attack Module

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Here we are creating a attacker node for sending the unwanted packet to their neighbour node. The neighbour node on receiving the unwanted packet capture the bandwidth of our network That means. in our contribution we set scan rate for spreading the infection , scan port by which port unwanted packet will be send , vulnerable node the node which can easily be effected (nearest neighbour node) , attack time particular time for spreading infection etc. And launch the DDOS attack, very first one vulnerable node receiver probing packet from attacker node and infected this node this infected node send probing packet to another neighbour node after some time number of nodes infected to our network.

Algorithem for DDoS attack module

Step1: Create attacker node;
Step2: Set attack rate 0.9;
Step3: Vulneribilty type;
Step4: Scan port 0;
Step5: Set vulnerable node; // node 3 ,9 ,17
Step6: Send probe pkt to any vulnerable node

```
While (node_rx_probe_pkt ==true)
                {
 infect node ;  // one node send probe pkt two another lonch DDOS attack
                }
```

Step7: Capture information after DDOS (event, time,send_id , Rx_id , protocol type,transport_info);

4.3. IDS (Intrusion Detection System)

In intrusion detection system firstly we performed simulation and check the normal and abnormal behaviour of the network according to parameter we set threshold level if information deviate more or less than 10 percentage so that network as infected and find the attacker node and block that node , so that in future no any intrusive process come to our network.

In example if we set as TCP sender node as S1 and Receiver Node R1 and intermediate node as I1, I2 and one IDS node that belong on the radio range of above declared node so here IDS check each packet sends by the sender which type of packet sends by the sender node and after that also analyse related path where the data packet come and forward, if any intermediate node modified the packet, IDS check which type of modification done on the packet it also check routing behaviour of each node if any node modify routing table so that IDS block the related misbehaviour nodes. We also analyse the behaviour through trace file and compare the result of normal case AODV routing time, DDOS time and IDS time and get the relative result of the network.

Algorithm for IDS (Intrusion Detection System) Module

Step1: Create node =ids :// set routing as IDSAODV
Step2: Set routing =AODV;
Step3: If (node in radio range)&&(nest hop !=Null)
{
Capture load(all_node);
Create normal_profile();
Create abnormal _table();
Step4: If(load<=max_limit)&&(new_profile==normal_profile())
{
No any attack;
}
Else
{
Attack in network;
If (new_attack==abnormal_table())
{
block the infected node;
}
Else
{
Insert Value into abnormal _table();
Find_attack_info();
}
}
Else
{
"node out of range or destination unreachable"
}
Step5: Find_attack_info()
{
Packet type;
Infection time;
Infected node;
Infection percentage;
}

4.4. DDOS and IDS Time Collaboration Diagram

Here we deploy in figure 4.1, collaboration at the time of DDOS and IDS module. Collaboration shows flow of event and interaction of each module according to event generation.

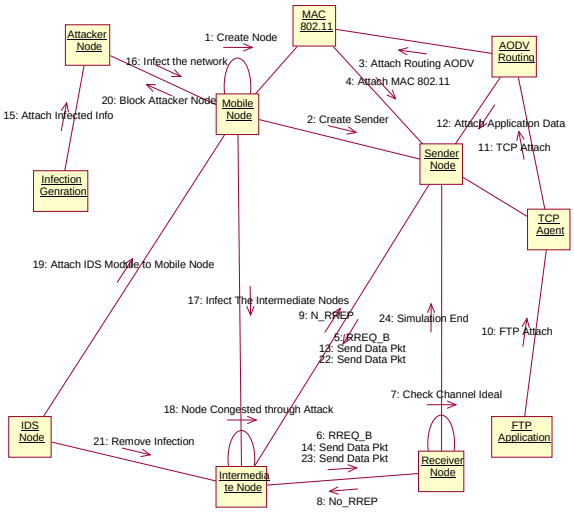

Fig. 1. Collaboration Diagram

5. Algorithm for Threshold

Step1: Set threshold (normal ± 10%);
Step2: If (abnormal ± 10% from Normal)
{
Can't block node;
}
Else { Block attack node;
Show abnormal info (event_type , pkt_type , infect_per,infect_node)
}

6. Simulation Parameter

Here we create the simulation parameter table, according to that given table we simulate the our result and analyze them. we use routing protocol as AODV with uni-casting mechanism and take the simulation time as 25 sec.

Sr. No.	Simulator parameter	Value
1.	No. of Nodes	30
2.	Dimension of simulated Area	800X600
3.	Routing Protocol	AODV ,IDS
4.	Simulation Time in seconds	25
5.	Transport Layer	TCP,UDP
6.	Traffic Type	FTP ,CBR
7.	Packet size (byte)	1000
8.	No. of Traffic Connection	20
9.	Maximum Speed (m/s)	25

Table 1. Simulation parameter

7. Simulation Details

The simulation described in this paper was tested using the ns-2 test-bed that allows users to create arbitrary network topologies [9]. By changing the logical topology of the network, ns-2 users can conduct tests in an ad

hoc network without having to physically move the nodes. ns-2 controls the test scenarios through a wireless interface, while the ad hoc nodes communicate through a wireless interface.

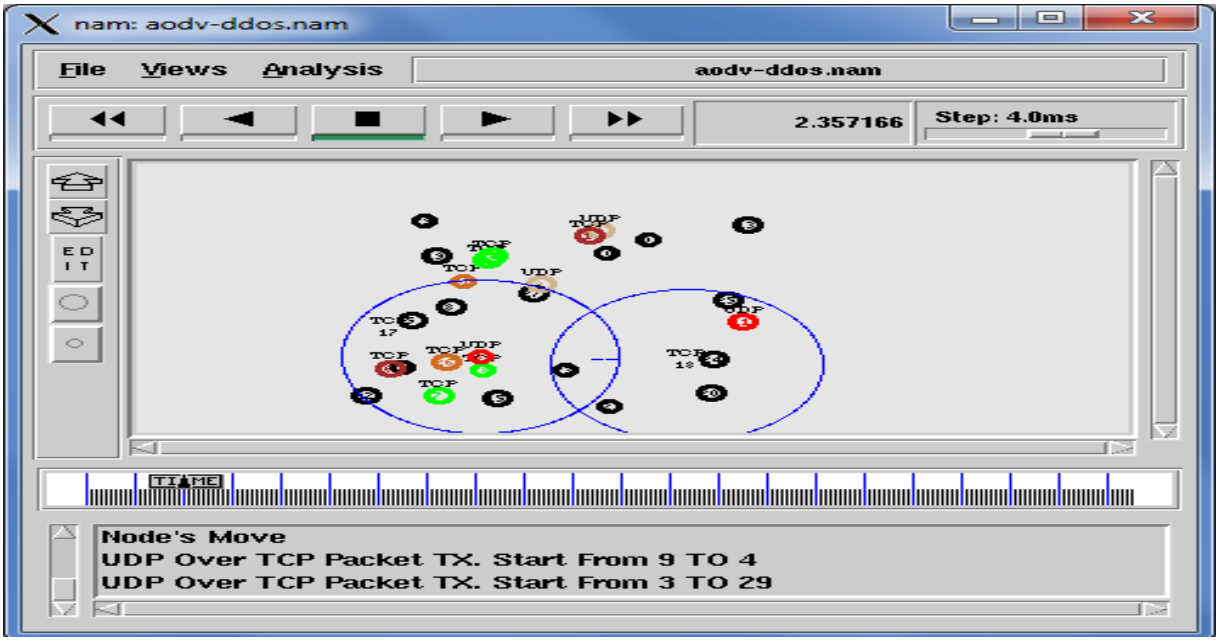

Fig 2. A sample topology generated by ns-2

In figure 2. we show sample topology with 30 mobile nodes and attack simulation, attacker node send the probing packet to all other neighbour and infect the network here node no 19, 3 and 11 are infected via ddos attack so that case our performance will decrease because actual data cant by sends through sender node, sender node send only routing packet but network are congested by unwanted packet.

8. Experimental Result

8.1. TCP Analysis at Normal Time

In our simulation we create five tcp connection and analyze them we find out if we set routing protocol as AODV and generate TCP connection with no infection of network so that our TCP performance is best. here we deploy tcp congestion window.

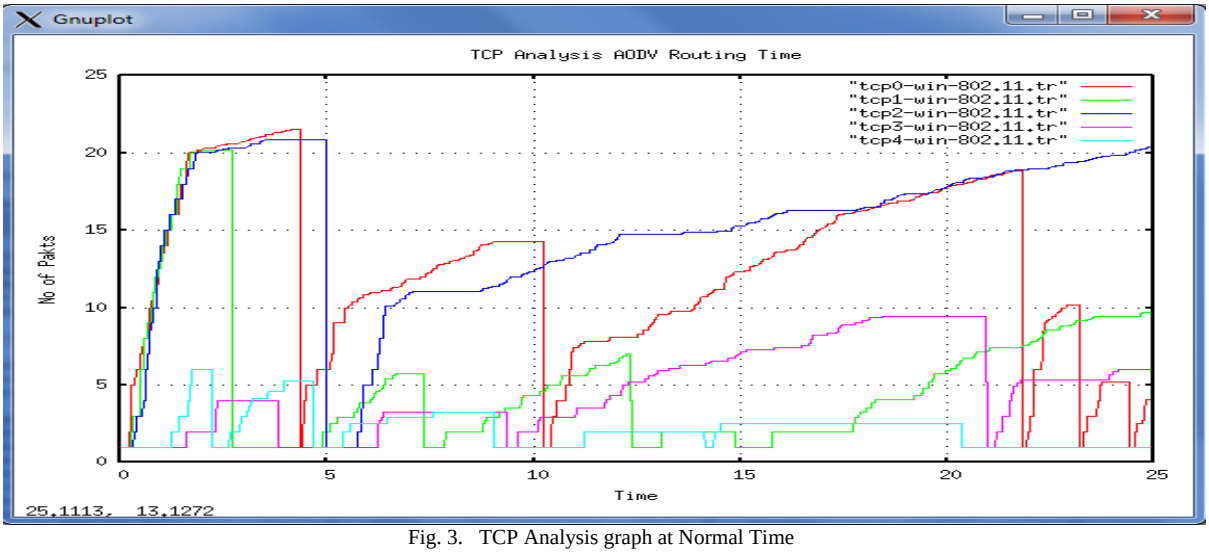

Fig. 3. TCP Analysis graph at Normal Time

8.2. TCP Analysis at DDOS Time

It is easy to interfere with wireless communications. A simple jamming transmitter can easily cause a DoS attack and provide communications impossible. In our simulation one node lunch DOS attack and spread over the network, if any node receives infected packet so that receiver nodes infected through attack and distribute

infected packet to other mobile node after some time maximum number of node infected and network performance minimize, here our tcp result is very poor as compare normal case.

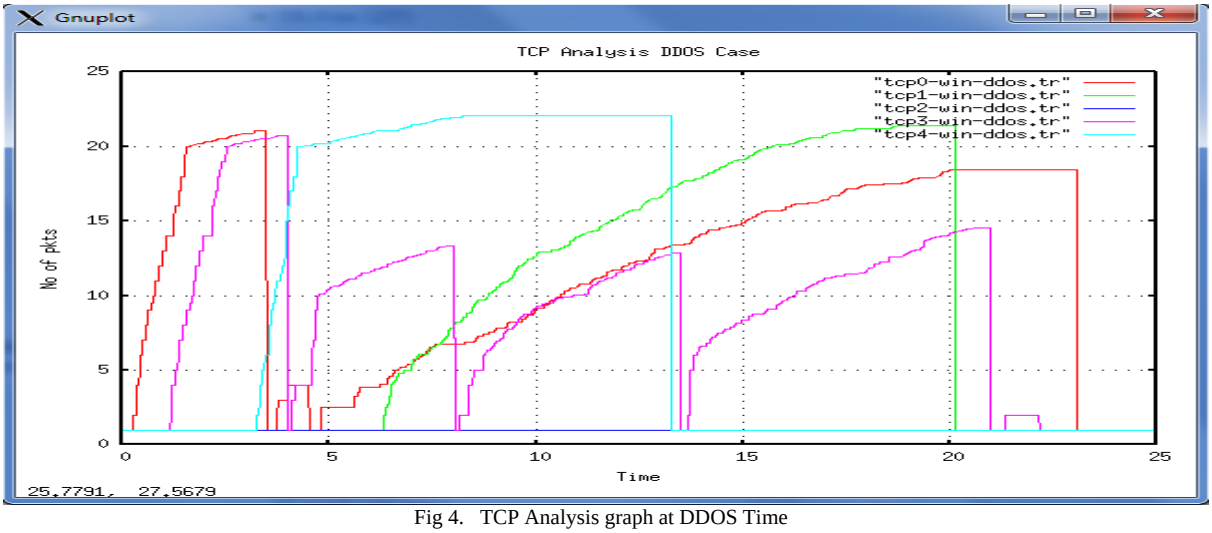

Fig 4. TCP Analysis graph at DDOS Time

8.3. TCP Analysis at DDOS and IDS Case

Here we analyze tcp window in both case DDOS and IDS case, if we deploy IDS in our network so attack percentage has minimized and our result has been improved.

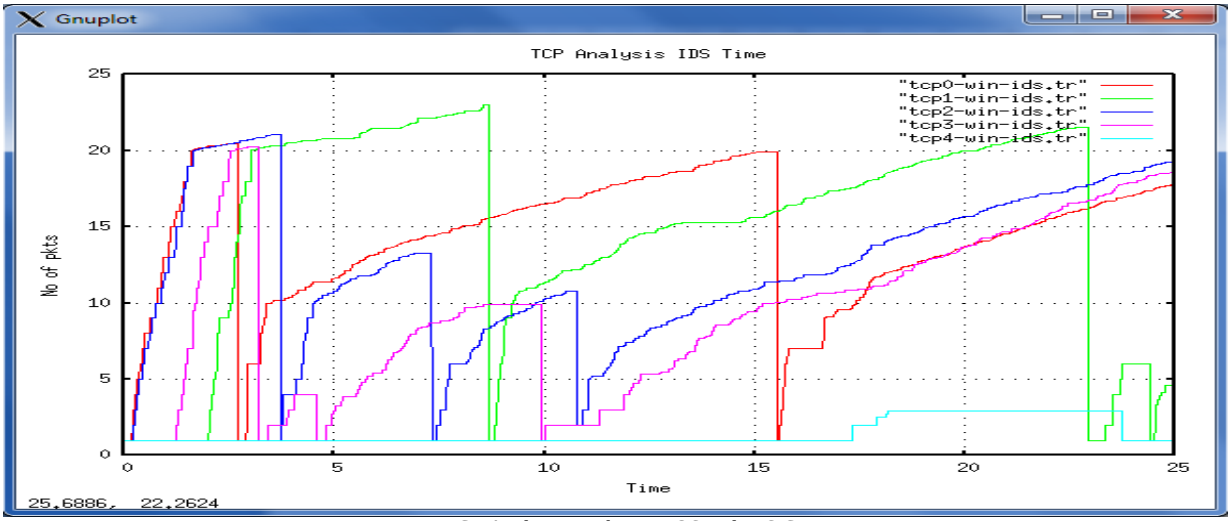

Fig 5. TCP Analysis graph at DDOS and IDS Case

8.4. Routing Load Analysis

The total number of routing packets transmitted during the simulation. For packets sent over multiple hops, each transmission of the packet or each hop counts as one transmission.

In our simulation normal and IDS time routing overhead is minimum but if DDOS attack comes onto the network so our routing overhead is maximize because attacker node consume network bandwidth and genuine sender can't sends data packet to actual receiver and send routing packet but can't find destination so routing overhead maximize and throughput minimize.

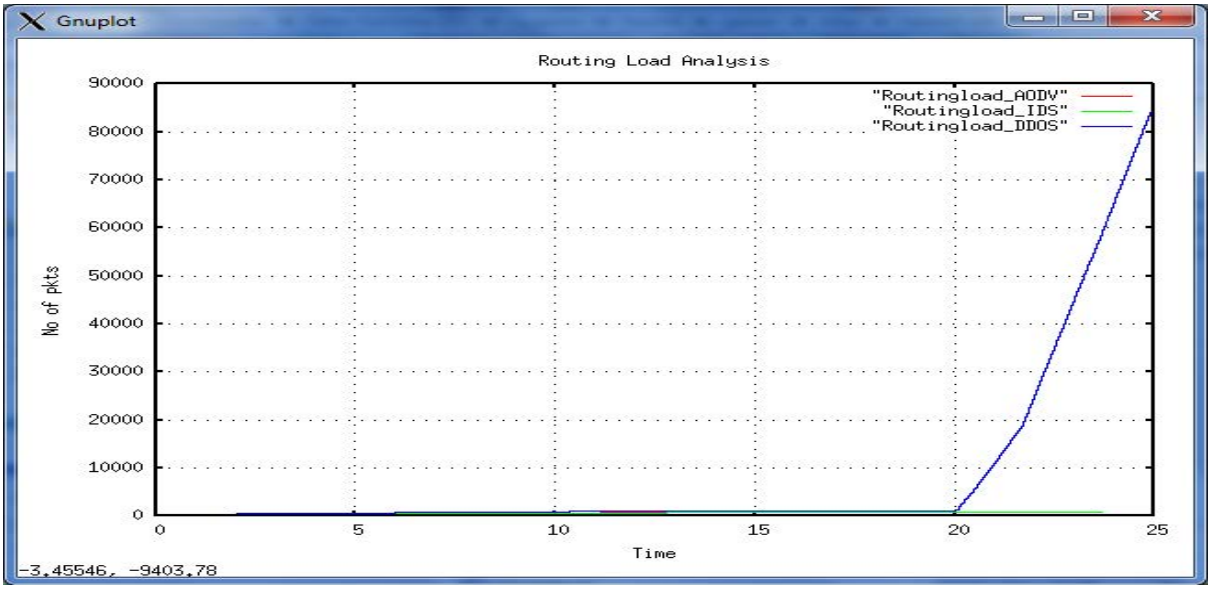

Fig 6. Routing Load Analysis

8.5. Packet Delivery Ratio Analysis

The ratio between the number of packets originated by the application layer CBR sources and the number of packets received by the CBR sink at the final destination. Here in AODV and IDS time packet delivery ratio result is very good but in case DDOS Attack after 21 sec. no any data packet transmission so PDR calculation ends.

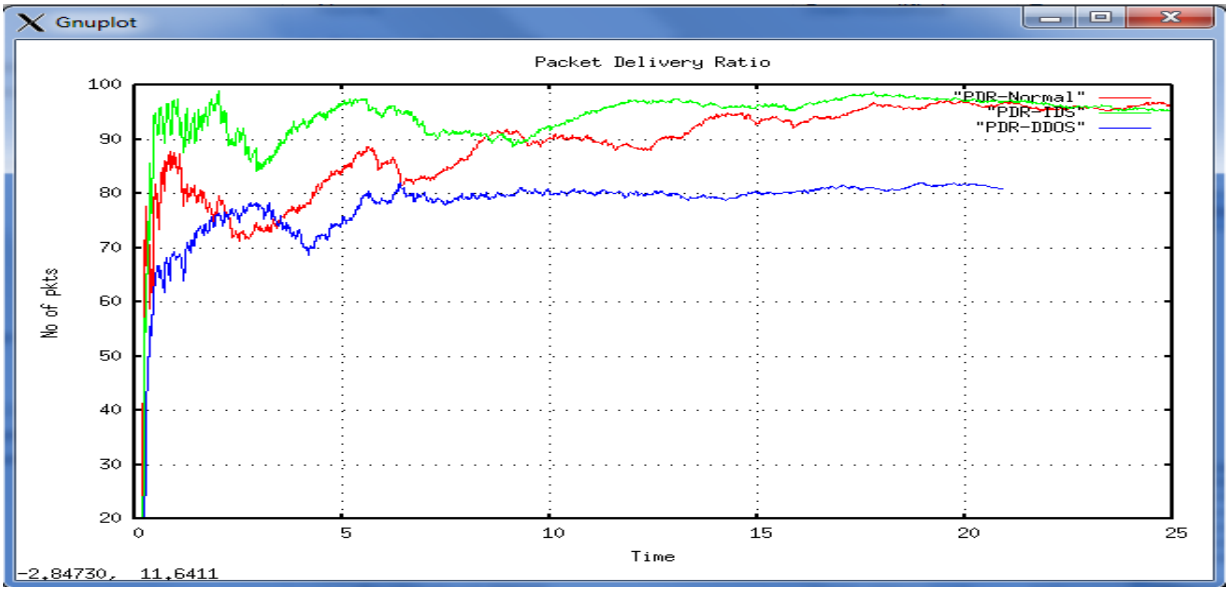

Fig 7. Packet Delivery Ratio Analysis

8.6. Analysis of packet sends and receives

In our simulation we generate FTP and TCP packet and analysis in the form of send/receive packet here result shows if we use IDS so our send/receive result is very good but the time of DDOS attack our data send and receives is very poor.

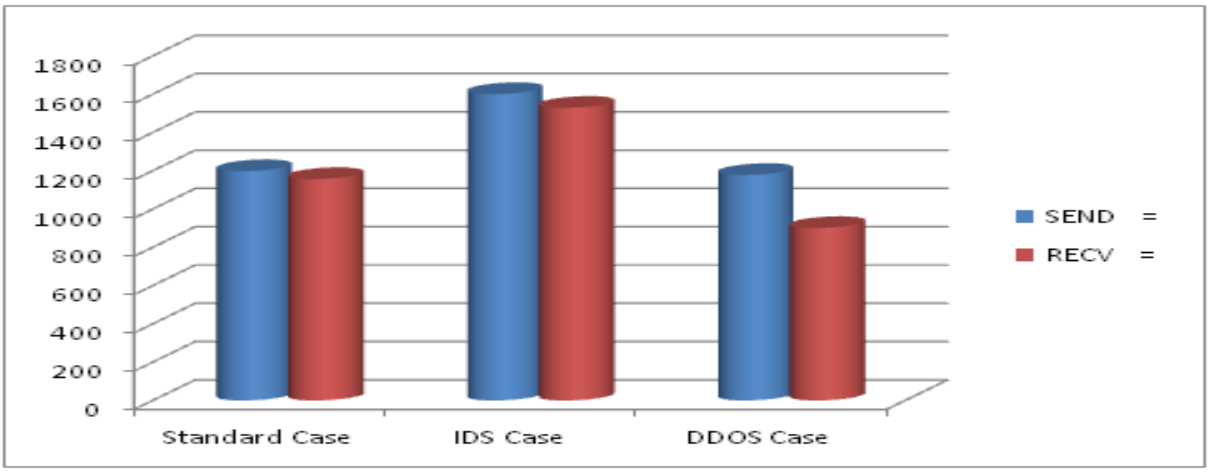

Fig 8. Analysis graph of packet sends and receives

9. Conclusion

We perform number of test in ns-2 simulator and analyse the result we get the summery result according to test simulation in normal routing time total number of packet received by the genuine receiver is 1157 but in case of attacker node packet receives 901 only that means 22% receiving decreases. But if we set one node as IDS so receiving percentage increases nearly 1529 that result concludes 32% percent increases. Other side also PDF packet delivery fraction analysis if attacker node comes on to the network so 20% PDF decrease. And IDS improve the PDF 19%. we also analyse routing overhead in normal case only 0.39 % of routing load but attacker node present case 122 times increase routing load, that means very–very routing over head increases it gives poor performance of the network, finally we conclude our result IDS (intrusion detection system) 99.9% data recover.

Overall Summery				
Parameter		**Standard Case**	**IDS Case**	**DDOS Case**
SEND	=	1198	1601	1178
RECV	=	1157	1529	901
ROUTINGPKTS	=	448	369	42991
PDF	=	96.58	95.5	76.49
NRL	=	0.39	0.24	47.71
Average e-e delay(ms)	=	691.45	331.75	685.09
No. of dropped data (packets)	=	40	66	234
No. of dropped data (bytes)	=	41920	68212	237600

Fig 9. Concluded Table

Here our system gives nearly 100% data recovery but one another research paper name as “Efficient Anomaly Intrusion Detection System in Ad-hoc Networks by Mobile Agents” detect only 80% and data recovery nearly 94% . Other paper “Behavior Based Anomaly Detection Technique to Mitigate the Routing Misbehavior in MANET” provide result in DSR case 77% , AODV case 60% and DSDV case nearly 50% misbehave detection.

10. Future Work

In This paper we simulate only one type attack (DDOS) and IDS in mobile ad-hoc network. In further We can also apply the other techniques like packet capturing, false route forwarding, changing source and destination addresses etc type of attack and protect through this different type of attack. In future we also simulate routing misbehaver module.

Mobile ad-hoc simulation is very big challenge in this day because ad-hoc network phases various challenges like infrastructure less network, no centralize control exists in future we simulate the result using number of parameter and improve the accuracy of our simulation.

Acknowledgments

Author are very thankful to the Samrat Ashok Technological Institute Vidisha (MP) India for supporting in contribution towards development of this Article

References

[1] S.A.Arunmozhi and Y.Venkataramani "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011

[2] L. Buttyan and J. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," ACM/Kluwer Mobile Networks and Applications (MONET) 8 (2003).

[3] M. Baker, E. Fratkin, D. Guitierrez, T. Li, Y. Liu and V. Vijayaraghavan, "Participation incentives for ad hoc networks," http://www.stanford.edu/~yl31/adhoc (2001).

[4] D. Barreto, Y. Liu, J. Pan and F. Wang, "Reputation-based participation enforcement for adhoc networks," http://www.stanford.edu/~yl314/adhoc (2002).

[5] S. Zhong, J. Chen and Y.R. Yang, "Sprite: A simple, cheatproof, credit-based system for mobile ad-hoc networks," Technical Report 1235, Department of Computer Science, Yale University (2002).

[6] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In: Mobile Computing and Networking. (2000) 255–265.

[7] S. Buchegger and J.Y.L Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Noes Fairness In Distributed Ad-hoc NeTworks," In Proc. Of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, IEEE (2002) 226–236.

[8] P. Michiardi and R. Molva, "Making greed work in mobile ad hoc networks," Technical report, Institut Eur´ecom (2002).

[9] The Network Simulator ns-2 http://www.isi.edu/nsnam/ns/

[10] A.D. wood and J.A. Stankovic, "Denial of Service in Sensor Networks," IEEE October 2002.

[11] J. Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, .A Secure Ad-hoc Routing Approach using Localized Self-healing Communities,. in *Proc. of ACM MobiHoc '05.*, 2005.

[12] Y. Hu, A. Perrig, and D. B. Johnson, .Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks,. in *Proc. of MobiCom '02*, Atlanta, USA, Sept. 2002.

[13] A. D. Wood and J. A. Stankovic, .Denial of Service in Sensor Networks,. *IEEE Computer Magazine*, vol. 35, no. 10, pp. 54.62, Oct 2002.

[14] S. Xu and T. Saadawi, .Revealing the Problems with 802.11 Medium Access Control Protocol in Multi-hop Wireless Ad Hoc Networks,. *Elsevier Journal of Computer Networks*, vol. 38, no. 4, pp. 531.548, 2002.

[15] G. Noubir and G. Lin, .On Link Layer Denial of Service in DATA Wireless LANs,. *Wiley Journal on Wireless Communications and Mobile Computing*, August 2004.

[16] F. Xing and W. Wang, .Modeling and Analysis of Connectivity in Mobile Ad Hoc Networks with Misbehaving Nodes,. in *Proc. of IEEE ICC '06.*, 2006.

[17] W. Q. Meeker and L. A. Escobar, *Statistical Methods for Reliability Data*. John Wiley and Sons Inc., 1998.

[18] D. Moore, C. Shannon, and J. Brown, .Code-Red: A Case Study on the Spread and Victims of an Internet Worm,. in *IMW '02: Proc. Of the 2nd ACM SIGCOMM Workshop on Internet Measurment*, 2002, pp. 273.284.

[19] F. Stevens, T. Courtney, S. Singh, A. Agbaria, J. F. Meyer, W. H. Sanders, and P. Pal, .Model-Based Validation of an Intrusion-Tolerant Information System,. in *Proc. of 23rd IEEE International Symposium on Reliable Distributed Systems (SRDS'04)*, Oct. 2004, pp. 184.194.