DETECTION AND RECTIFYING VARIOUS ATTACKS IN MULTIHOP NETWORKS

A.V.Sindhuja[1], R.Sarath kumar [2], R.V.Naveen Kumar[3] , K.Chitra[4]

[1]*Assistant Professor, Department of Electronics and Communication Engineering, MNM Jain Engineering College, Chennai 600097, India.*
[2]*PG Student, Department of Electronics and Communication Engineering, Sathyabama Institute Of Science And Technology, Chennai 600119, India.*
[3] *UG Student, Department of Computer and Science Engineering, St.Peter's Institute Of Higher Education And Research, Chennai 600054, India.*
[4] *UG Student, Department of Electronics and Communication Engineering, MNM Jain Engineering College, Chennai 600097, India.*

ABSTRACT

Stealthy attacks were considered as a kind of dangerous attack because a small number of malicious parties can easily ruin the entire network performance. The most possible attacks were misrouting, power control, identity delegation, colluding collision, data modification and denial of service. Stealthy packet dropping disrupts the packet from reaching the destination through malicious behavior at an intermediate node. The malicious node gives the impression to its neighbors that it performs the legitimate forwarding action. Moreover, a legitimate node comes under suspicion. A popular method for detecting attacks in wireless networks is behavior based detection performed by normal network nodes through overhearing the communication in their neighborhood. this project provides a protocol namely MAAM to detect and isolate stealthy packet dropping attack efficiently .it performs effectively because by maintaining extra neighbours in the monitoring process and accurately identifies the malicious user. MAAM presents two techniques that can be overlaid on basic local monitoring: having the neighbors maintain additional information about the routing path, and adding some checking responsibility to each neighbor. Additionally, MAAM provides an innovative mechanism to better utilize local monitoring by considerably increasing the number of nodes in a neighborhood that can do monitoring. We show through analysis and simulation experiments that basic local monitoring fails to efficiently mitigate most of the presented attacks while MAAM successfully mitigates them.

Keyword: - *MAAM,* PRNETs,

1. INTRODUCTION

1.1 Wireless Ad-hoc Network

A wireless ad hoc network is a decentralized type of wireless network The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks. It also refers to a network device's ability to maintain link status information for any number of devices in a 1 link (aka "hop") range, and thus this is most often a Layer 2activity. Because this is only a Layer 2 activity, ad hoc networks alone may not support a routable IP network environment

without additional Layer 2orLayer 3capabilities.The earliest wireless ad hoc networks were the "packet radio" networks (PRNETs) from the 1970s, sponsored by DARPA after the ALOHA net project

1.2 Ad-hoc Networks

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security. The security hole provided by Ad-hoc networking is not the Ad-hoc network itself but the bridge it provides into other networks, usually in the corporate environment, and the unfortunate default settings in most versions of Microsoft Windows to have this feature turned on unless explicitly disabled. Thus the user may not even know they have an unsecured Ad-hoc network in operation on their computer. If they are also using a wired or wireless infrastructure network at the same time, they are providing a bridge to the secured organizational network through the unsecured Ad-hoc connection. Bridging is in two forms. A direct bridge, which requires the user actually configure a bridge between the two connections and is thus unlikely to be initiated unless explicitly desired, and an indirect bridge which is the shared resources on the user computer. The indirect bridge provides two security hazards. The first is that critical organizational data obtained via the secured network may be on the user's end node computer drive and thus exposed to discovery via the unsecured Ad-hoc network.

The second is that a computer virus or otherwise undesirable code may be placed on the user's computer via the unsecured Ad-hoc connection and thus has a route to the organizational secured network. In this case, the person placing the malicious code need not "crack" the passwords to the organizational network, the legitimate user has provided access via a normal and routine log-in. The malfactor simply needs to place the malicious code on the unsuspecting user's end node system via the open (unsecured) Ad-hoc networks.

1.3 Security Issues and Solutions

ATTACK NAME	ATTACK DESCRIPTION	ATTACK INSTANTIATION REQUIREMENT
misrouting	relays the packet to wrong next hop	one compromised node in the route between the sender and receiver
power control	controls the transmission to exclude next hop	one compromised node in the route between sender and receiver with power control capability
colluding collision	simultaneous transmission to create a collision at the next hop	one compromised node in the route between the sender and receiver and one external attacker node close to the next-hop from the compromised node
identity delegation	delegate the relay responsibility to a colluding partner close to the sender	one compromised node in the route between the sender and receiver and one external attacker node close to the compromised node
denial of services	renders a network host or other piece of network infrastructure unusable by legitimate users	once a compromised source host has been identified it is quarentied it is a slow process
data modification	data get modified in destination node from source node	once the gnode gets data modified details it retransmit the data

Table -1

1.4 Stealthy Packet Dropping Attacks:

We distinguish between an external malicious node, which does not possess the cryptographic keys in the network, and an internal compromised node, which does and is created by compromising an erstwhile legitimate node. Consider a scenario in which a node called S is forwarding a packet to a compromised node called M. M is supposed to relay the packet to the next-hop node D. The first form of the attack is called packet misrouting. In this mode, M relays the packet to an incorrect next-hop neighbor. The result is that the packet does not reach its intended next-hop(D) while M appears to the guards as doing its forwarding job correctly.

The second mode is called the power control attack. In this mode, M controls its transmission power to relay the packet to a distance less than the distance between M and D. Therefore, the packet does not reach the next-hop while the attacker avoids detection by many guards. The third form of the attack is called the colluding collision attack. In this mode, the attacker uses a colluding node (external or internal) in the range of D to transmit data at the same time when M starts relaying the packet to D. Therefore, a collision occurs at D, which prevents the packet from being correctly received by D, while M appears to be performing its functionality correctly. The final mode of stealthy packet dropping is called the identity delegation attack. In this mode, the attacker colludes with a node E placed close to the source node S. E is allowed to use M's identity and transmit the packet. Since E is almost at the same place as S, D does not receive the packet while the guards of M are deceived that M relays the packet to the next-hop. In each of these attack types, the adversary can successfully perform the attack without detection through BLM. Additionally, in each attack type, a legitimate node is accused of packet dropping. We provide a protocol called MAAM (MAJOR PACKET ATTACKS IN AD HOC NETWORKS: DETECTION AND RECTIFYING).

2. RELATED WORK

2.1 Stealthy attacks in wireless ad hoc networks:

Detection and counter measure (2010). Stealthy packet dropping is a suite of four attacks *viz*. misrouting, power control, identity delegation and colluding collision that can be easily launched against multihop wireless ad hoc networks. We show that local monitoring, and the wider class of overhearing-based detection, cannot detect stealthy packet dropping attacks. Additionally, it mistakenly detects and isolates a legitimate node. we present a protocol called sadec that can detect and isolate stealthy packet dropping attack. We have introduced a new class of attacks called stealthy packet dropping which disrupts a packet from reaching the destination by malicious behavior at an intermediate node. this can be achieved through misrouting, controlling transmission power, malicious jamming at an opportune time, r identity sharing among malicious nodes we showed that basic local monitoring (blm) based detection cannot detect these attacks. Additionally, it will cause a legitimate node to be accused. We then presented a protocol called sadec that successfully mitigates all the presented attack. sadec builds on local monitoring and requires nodes to maintain additional routing path information and adds some checking responsibility to each neighbor. we showed through analysis and simulation that blm fails to mitigate most of the presented attacks while sadec successfully mitigates them. the improvement is seen in terms of increase in the probability of isolation of malicious nodes and decrease in the probability of isolation of legitimate nodes. in future work, we are considering detection techniques for multichannel multi-radio wireless networks. The listening activity for detecting malicious behavior is more complicated due to the presence of multiple channels and multiple radios. We also plan to analyze the impact of the detection technique on the network throughput under different adversary models.

2.2 Mispar:

Mitigating stealthy packet dropping in locally-monitored multi-hop wireless ad hoc networks (2008).local monitoring has been demonstrated as a power full technique for mitigating security attacks in multi-hop ad-hoc networks. In local monitoring, nodes overhear partial neighborhood communication to detect misbehavior such as packet drop or delay. local monitoring as presented in the literature is vulnerable to a class of attacks that we introduce here called stealthy packet dropping. stealthy packet dropping disrupts the packet from reaching the destination by malicious behavior at an intermediate node we provide a protocol called mispar based on local

monitoring to remedy each attack. it presents two techniques – having the neighbors maintain additional information about the routing path, and adding some checking responsibility to each neighbor. We show through analysis and simulation that the basic local monitoring fails to mitigate any of the presented attacks while mispar successfully mitigates them the malicious behavior cannot be detected by any behavior-based detection scheme presented to date. Specifically, additionally, it will cause a legitimate node to be accused. We then presented a protocol called mispar based on local monitoring to remedy each attack. the solution takes two forms – having nodes maintain additional routing path information, and adding some checking responsibility to each neighbor..in future work, we are considering detection techniques for multi-channel wireless networks. The listening activity for detecting malicious behavior is more complicated due to the presence of multiple channels. We also plan to analyze the impact of the detection technique on the network throughput

3. SYSTEM DESIGN

3.1 Aim And Objective

- To detect and to isolate stealthy packets from normally delivered packets.
- To efficiently isolate stealthy packets dropping attacks
- To provide and innovative mechanism to better utilize local monitoring.

3.2 Block Diagram

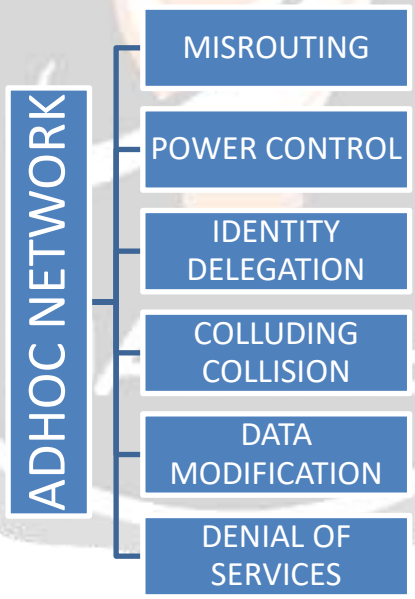

Chart -3.1 Overall block diagram for adhoc network

3.3 Program Flow

In our simulation setup has 2 GNODE (indicating by blue color) and each GNODE has 6 client nodes (indicating by red color) & both GNODE is connected through switch.

There are six network attacks in our simulation.

i. Misrouting
ii. Drop through power control

iii. Colluding collision
iv. Identity delegation
v. Data modification
vi. Denial of Service Attack

3.4 Program Flow Chart

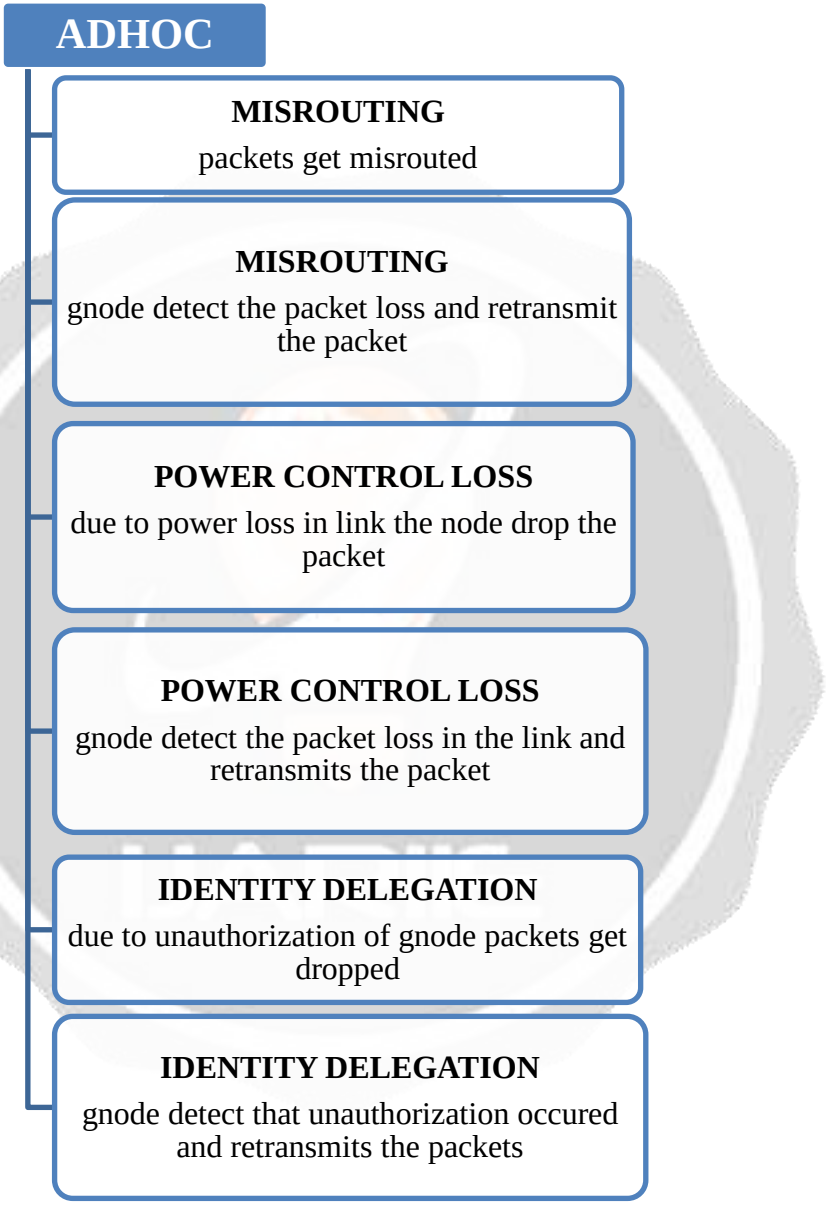

Chart-3.2

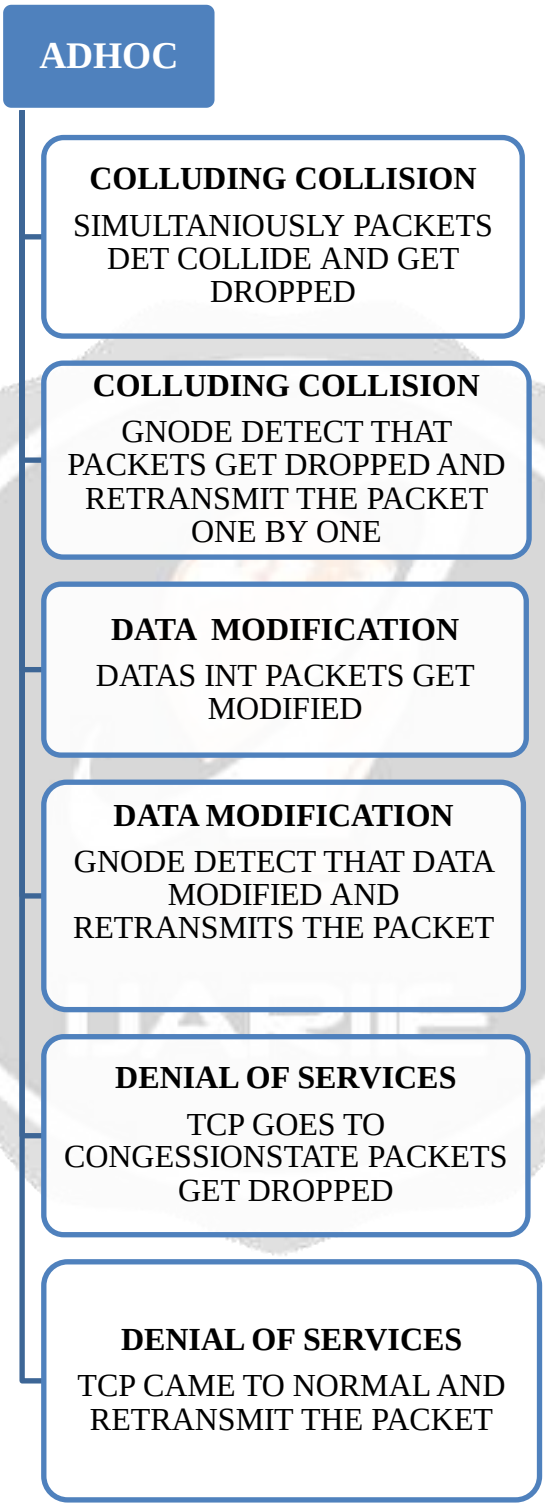

Chart-3.3

4. RESULTS AND DISCUSSION

4.1 Misrouting

In this routing node2 is forwarding a packet to a compromised node called node9. But node9 is supposed to relay the packet to the next-hop node node10. GNODE detect the misrouting situation so retransmit the same frame to node9.

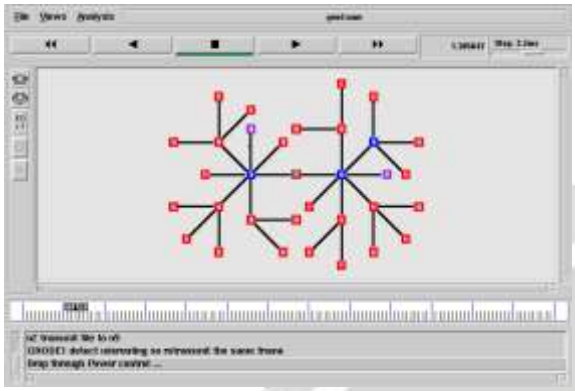

Fig-4.2.Retransmission occur in misrouted nodes

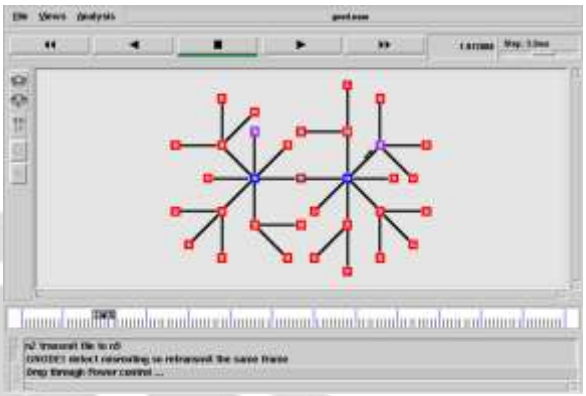

Fig.-4.1.Misrouting occur

4.2 Drop Through Power Control

In this node4 transmit the ftp file to node12.during that time the power loss all packets are dropped. After that GNODE2 detect power recover, then it send request to retransmit the same frame to GNODE1.so node4 retransmit that the same frame node4 to node12

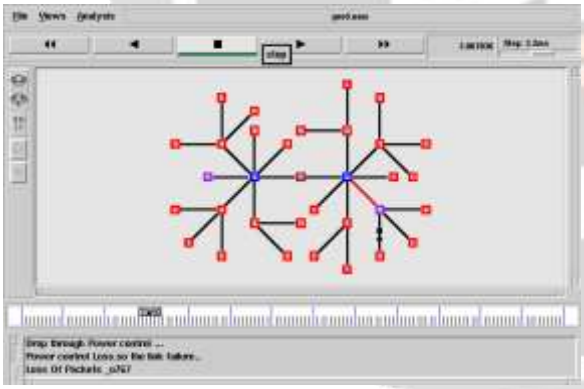

Fig-4.3 Packet loss occur due to power loss

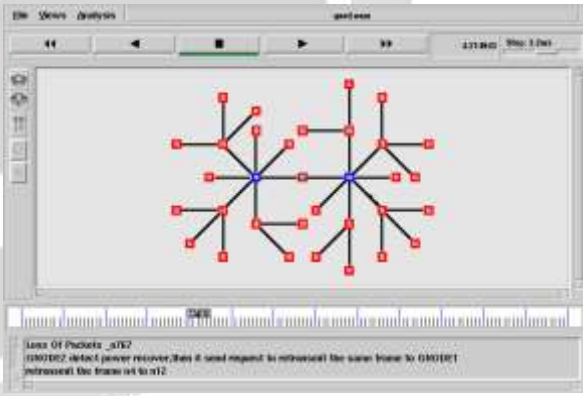

Fig-4.4 Retransmission occur

4.3 Colluding Collision:

Node3 ----------> node 11 and node13 ----------> node1 are Simultaneous transmission to create a collision at the next hop. Both GNODE detect data collision so separately once analyses the transmit line.

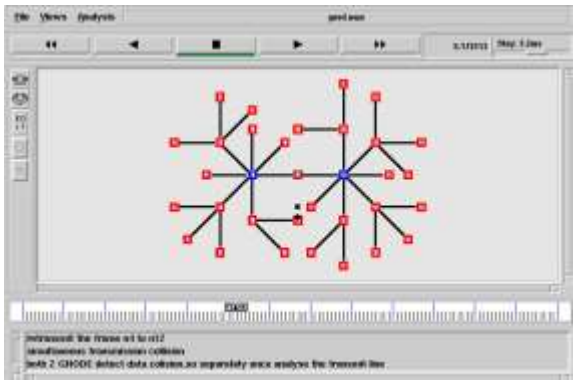

Fig-4.5 Collision colluding leads to packet loss

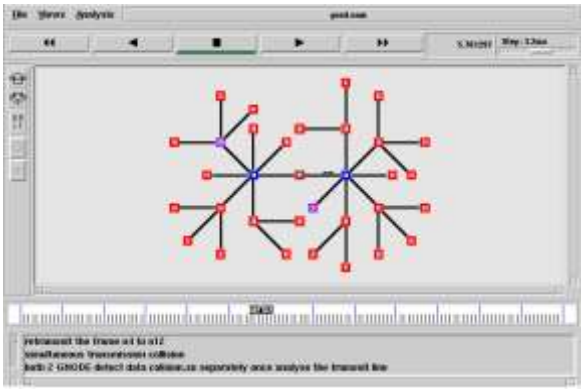

Fig-4.6 One by one retransmission occur

4.4 Identity Delegation:

Malicious occurs in both GNODE. Authority missing in incoming packets so GNODE drop the packets.

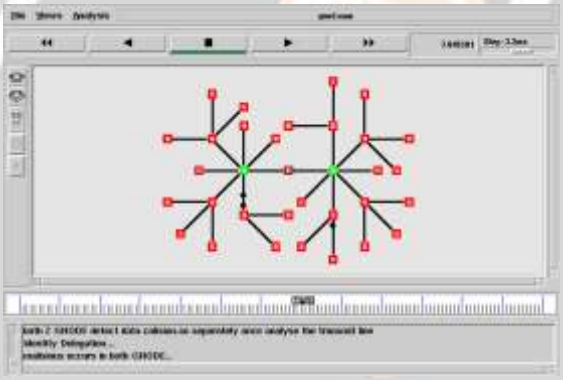

Fig- 4.7 Authentication missing loss the data packets and gnode retransmittts the data packets

4.5 Data Modification:

In this node8 transmit a ftp file to node6.but node6 received only the modified data. GNODE detects the data modification. So retransmit the same frame

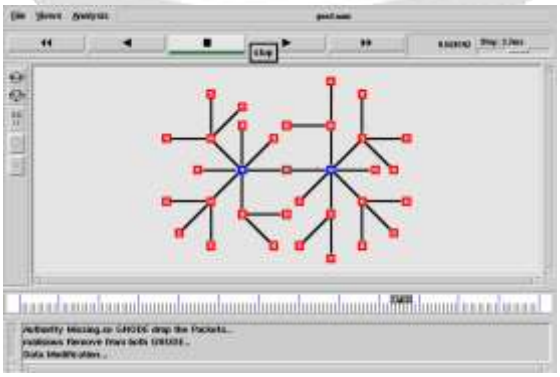

Fig.-4.8 Node receives the modified data

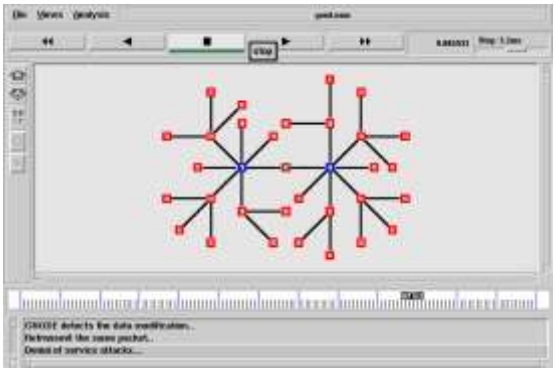

Fig.-4.9 Retransmission occur and correct data is transmitted

4.6 Denial Of Service

Due to the packet forwarding the TCP goes to congestion state, then tcp came to normal stage.

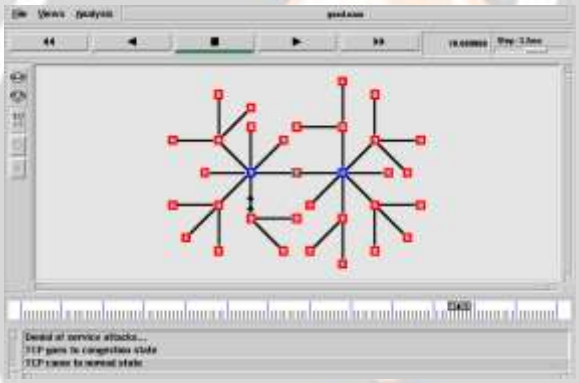

Fig.-4.10.Denial of services occur

4.7 Trace Data Analysis:

Trace file is used to trace the number of packets transmitted respective to the time

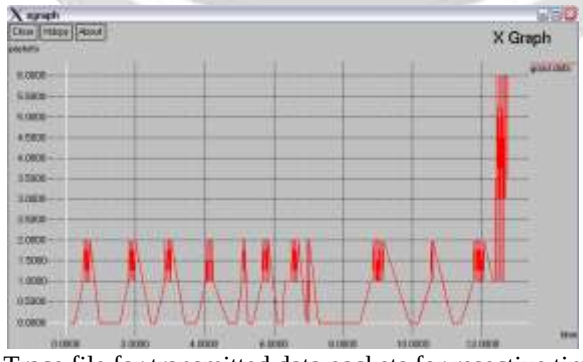

Fig-.4.11. Trace file for transmitted data packets for resective time is given

5. CONCLUSION

Thus the major packet attacks were mitigated and rectified themselves by GNODE special properties and it is done and verified by using ns2(network simulator 2) which used for programing the mitigation flow and rectifying them in adhoc network.in future we are going to mitigate and rectify the major packet attacks in multi channel radio networks using this MAAM(MAJOR PACKET ATTACKS IN ADHOC NETWORKS: DETECTION AND RECTIFYING) protocol

6. REFERENCES

[1] stealthy attacks in wireless ad hoc networks: detectionand countermeasure
issakhalil and saurabhbagchi(2010)
[2]MISPAR: mitigating stealthy packet dropping in locally-monitored multi-hop
wireless ad hoc networks issaKhalil college of information technologyunited arab emirates university, uae email: ikhalil@uaeu.ac.aesaurabhbagchidependable computing systems lab (dcsl)school of electrical & computer engineeringpurdue university, usaemail: sbagchi@purdue.edu
[3]MOBIWORP: mitigation of the wormhole attack in mobile multihop wireless networks issakhalil, saurabhbagchi, ness b. shroff dependable computing systems lab and center for wireless systems and applications (cwsa)school of electrical & computer engineering, purdue university465 northwestern avenue, west lafayette, in 47907.email: {ikhalil, sbagchi, shroff}@purdue.edu ph. 765-494-3362
[4] A. A. Pirzada and C. McDonald, "Establishing Trust In Pure Ad-hoc Networks," in ACSC 04, 26(1), pp. 47-54, 2004.
[5] S. Buchegger, J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes-Fairness in Distributed Ad-hoc NeTworks," in MOBIHOC'02, pp. 80-91, 2002.
[6] Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," in Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pp. 135-147, 2003.
[7] Y. C. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," ACM Workshop on Wireless Security (WiSe'03), pp. 30-40, 2003.
[8] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense againstwormhole attacks in wireless networks," in INFOCOM, pp. 1976-986, 2003.
[9] I. Khalil, S. Bagchi, and N. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," inDSN'05, pp. 612-621, 2005.
[10] I. Khalil, S. Bagchi, and N. B. Shroff, "MOBIWORP: Mitigation of theWormhole Attack in Mobile Multihop Wireless Networks," Elsevier Ad hoc

Networks Journal, V. 6, Issue 3, pp. 344-362, May 2008.
[11] I. Khalil, S. Bagchi, C. Nina-Rotaru, and N. Shroff, "UNMASK: UtilizingNeighbor Monitoring for Attack Mitigation in Multihop Wireless Sensor Networks," in Elsevier Ad Hoc Networks Journal, V. 8, I. 2, pp. 148-164, 2010.
[12] S.J. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," in IEEE International Conference on Communications (ICC), pp. 3201-3205, 2001.
[13] Q. Zhang, P. Wang, D. Reeves, and P. Ning, "Defending against Sybil Attacks in Sensor Networks," SDCS 2005, pp. 185-191, 2005.
[14] C. Basile, Z. Kalbarczyk, and R. K. Iyer, Neutralization of Errors and Attacks in Wireless Ad Hoc Networks, DSN'05, pp. 518-527, 2005.
[15] B. Carbunar, I. Ioannidis and C. Nita-Rotaru, JANUS: Towards Robust andMalicious Resilient Routing in Hybrid Wireless Networks, WiSe'04, pp. 11-20,2004.
[16] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru and H. Rubens,"ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol forWireless Ad Hoc Networks," ACM Transactions on Information and SystemSecurity (TISSEC), V. 10, Issue. 4, 2008.
[17] R. Molva, G. Tsudik, and D. Westhoff (Eds.), "Statistical Wormhole Detection in Sensor Networks," ESAS'05, LNCS 3813, pp. 128–141, 2005.
[18] D. Liu and P. Ning, "Establishing Pair-wise Keys in Distributed SensorNetworks," in the ACM Conference on Computer and Communications
Security (CCS), pp. 52-61, 2003.

[19] D. Johnson, D. Maltz, and J. Broch, The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks, Ad Hoc Networking, Addison-Wesley, 2001.
[20] C. E. Perkins and E. M. Royer, Ad-Hoc On-Demand Distance Vector Routing, in Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 90-100, 1999.
[21] D. Ganesan, B. Krishnamurthy, A.Woo, D. Culler, D. Estrin, and S. Wicker. An empirical study of epidemic algorithms in large scale multihop wireless networks. Technical Report IntelIRP-TR-02-003, Intel Research, March 2002.