Performance Analysis of MANET Reactive Routing under Security

K Sreenivasulu
Professor & HOD-CSE
Madina Engineering College
KADAPA, A.P, INDIA

E V Prasad, PhD.
Rector,
JNTUK
KAKINADA, A.P, INDIA

A. Subramanyam, PhD.
Professor & HOD-CSE
AITS
RAJAMPET, KADAPA, A.P

ABSTRACT

Security is an essential service for wired and wireless network communications. The success of mobile ad hoc networks (MANET) mainly depends on people's confidence in its security. In a MANET, a collection of mobile hosts with wireless network interfaces form a network without the aid of any fixed infrastructure or centralized administration. The characteristics of MANET pose challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. There are a wide variety of attacks that target the weakness of MANET, and Black-hole attack and Denial of Service attack (DOS) are the most prominent among this. Most of the research is focused on detect and how avoid these attacks by compromising on the performance of the network. This paper considers network Quality of Service (QoS) has one of the prime important factor and with the Overhead and packet-Delivery are the two important criteria evaluate the performance of the network in the presence of the security attacks..

Keywords : MANET, QOS, AODV, Security Attacks.

1. INTRODUCTION

A mobile ad hoc network (MANET) is a group of devices or nodes that transmit across a wireless communication medium. Cooperation of nodes is essential to forward packets on behalf of each other when destinations are out of their direct wireless transmission range as there is no centralized control or network infrastructure for a MANET and hence its deployment is quick and inexpensive. The nodes ability to move freely ensures a flexible and versatile dynamic network topology which is another important feature of a MANET. Some of the MANET applications includes emergency disaster relief, military operations over a battlefield (vulnerable infrastructure), and wilderness expeditions (transient networks), and community networking and interaction between students during a lecture.

The major characteristics of MANET include

1.1 Cooperation:

If the source node and destination node are out of range with each other then the communication between them takes place with the cooperation of other nodes such that a valid and optimum chain of mutually connected nodes is formed. This is known as multi-hop communication. Hence each node is to act as a host as well as a router simultaneously.

1.2 Dynamism of Topology*:*

The nodes of MANET are randomly, frequently and unpredictably mobile within the network. These nodes may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity of routing. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes.

1.3 Lack of fixed infrastructure:

The absence of a fixed or central infrastructure is a key feature of MANETs. This eliminates the possibility to establish a centralized authority to control the network characteristics. Due to this absence of authority, traditional techniques of network management and security are scarcely applicable to MANETs.

1.4 Resource constraints:

MANETs are a set of mobile devices which are of lower limited power capacity, computational capacity, memory, bandwidth etc. by default. So in order to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring.

All of the routing protocols in MANETs depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The basic assumption in such a setup is that all nodes are well behaving and trustworthy. Albeit in an event where one or more of the nodes turn malicious, security attacks can be launched which may disrupt routing operations or create a DOS (Denial of Service) condition in the network. Because of the lack of the centralized authority, less distributed infrastructure and dynamic nature of nodes, the ad hoc networks are vulnerable to various kinds of security attacks. The challenges to be faced by MANETs are over and above to those to be faced by the traditional wireless networks. The accessibility of the wireless channel to both the genuine user and attacker make the MANET susceptible to both passive eavesdroppers as well as active malicious attackers.

2. IMPORTANCE OF QUALITY OF SERVICE

Assuring the QoS mobile wireless multi-hop networks such as MANETs is very challenging compared to wired networks because of various difficulties associated with these types of networks. The major issues that still pose challenges for MANETs include :

2.1 Limiting the Capacity Constraints:

Clients in multi-hop wireless networks are generally equipped with a single wireless interface only, further limiting the communications capacity of these nodes.

2.2 Unreliable Communication Medium:
The wireless medium used for communication in multi-hop wireless networks is prone to errors due to interference noise generated from transmissions of other wireless devices in the vicinity as well as multi-path fading effects.

2.3 Unpredictable Channel Access Delay:

Calculating and guaranteeing tight delay bounds generally required for real-time communication.

2.4 Inaccurate Bandwidth Estimation:
Available wireless channel bandwidth at a mesh client or router is difficult to accurately determine, as it is affected by a number of factors, including the traffic load in the wireless transmission , sensing range, node mobility, as well as the general variability of wireless links.

2.5 Dynamic Topology and Mobility:
The client nodes in multi-hop wireless networks are generally mobile, resulting in routing information to become stale relatively quickly.

2.6 Absence of Centralized QoS Control:
QoS provisioning has to be done in a distributed fashion, which is much more challenging than for a centralized network.

2.7 Network Heterogeneity:
Another key challenge in QoS provisioning is the high level of heterogeneity present in multi-hop wireless networks. Mesh routers differ from mesh clients considerably in terms of level of mobility as well resource availability.

3. SECURITY ATTACKS

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET.

Table 1 shows the general taxonomy of security attacks against MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

The attacks can also be classified into two categories, namely external attack sand internal attacks, according the domain of the attacks also known outsider and insider attacks [9]. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

Table 1: Security Attacks Classification

1	Passive Attacks	Eavesdropping, traffic analysis, monitoring
2	Active Attacks	Jamming, spoofing, modification, replaying, DoS

Black Hole Attack and Denial of Service Attack are the two major active attacks by Sudhir Agrawal [2].

Black Hole Attack:

In this attack, the attacker node injects false route replies to the route requests claiming to have the shortest path to the destination node whose packets it wants to intercept. Once the fictitious route has been established the active route is routed through the attacker node. The attacker node is then in a position to misuse or discard any or all of the network traffic being routed through it.

In black-hole attack, the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow is forward any packet anywhere. This attack is called a black-hole as it swallows all data packets. In figure 1, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node which acts as a black-hole. The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from S towards M instead of D.

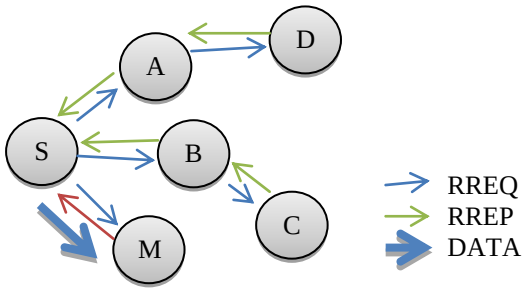

Fig1: Black-hole Attack

The Denial of Service attacks on network layer generally fall into three categories: resource deprivation, routing disruption, and forwarding rejection.

In a resource deprivation attack, malicious nodes can inject extra control or data packets into the network. For example, if AODV is used for a MANET, a malicious node may keeps ending different RREQ messages to its neighbors. Since the sequence numbers or fake destination addresses can be changed each time, an attacker's neighbors are not able to discern if these messages are fake ones or new requests, such that they have to forward to their neighbors and so forth. If the malicious node sends these fake messages at a high rate, its neighbors have to spend much resources, such as bandwidth, CPU cycles, and battery energy, to handle these fake messages.

A slightly less aggressive version of this attack was presented J. Kong, X. Hong[9] where a malicious node keeps initiating route discovery requests at a lower rate but ignores any reply to them. Besides the control packet flooding attack, a malicious node can also inject a large number of junk data packets into the route to consume the resource of intermediate routing nodes.

Q. Gu, P. Liu, S. Zhu [8] studied this attack and proposed an on-demand and hop-by-hop source authentication protocol in

forwarding packets, so called SAF, to mitigate this attack. In a route disruption attack, malicious nodes may send forged routing packets to mislead the route selection

In Rushing attack introduced by Yih-Chun Hu [5]. a malicious node disseminates RREPs faster than other nodes. When cooperative nodes receive the later arrived RREPs, they will treat these legitimate RREQs as the duplicates and drop them. they presented a rushing attack prevention have protocol a to thwart this attack.

Compared with the resource deprivation and route disruption attack, malicious nodes launching forwarding rejection attacks may comply with all routing procedures.

The Jellyfish attack was introduced and studied thoroughly in Aad, J.-P. Hubaux [6]. A malicious node launching Jellyfish attacks may keep active in both route discovering and packet forwarding in order to prevent it from detection and diagnosis, but the malicious node can attack the traffic via itself by reordering packets, dropping packets periodically, or increasing jitters. The Jellyfish attack is especially harmful to TCP traffic in that cooperative nodes can hardly differentiate these attacks from the network congestion. Malicious nodes may even abuse directional antenna and dynamic power techniques to avoid upstream nodes to detect their misbehaviors of dropping packets

A concept of self-healing community J. Kong, X. Hong [9] was claimed to be able to mitigate the directional and dynamic power transmission attack, which requires the network interface stay in the promiscuous mode; however, in military ad hoc networks, setting network interface cards as the promiscuous mode enables nodes to become sniffers or eavesdroppers, which may lead to other potential security threats.

Some of the above authors have only observed the impact of the attacks on the network and not initiated any type of analysis on the network performance.

4. SIMULATION ANALYSIS

Ns-2 simulator is used for analysis of network performance in terms of overhead and packet delivery, under black-hole and DoS attacks.

The simulation parameters are as follows:

Table 2: Simulation Parameters

Simulator	NS-2
Network Area	3000x1000 m^2
Network Density	50, 100, 150, 200
Number of Attackers	4, 8, 12, 16
Attacks	Blackhole, DOS
Base Routing Protocol	AODV
Performance parameters	Overhead, Packet delivery

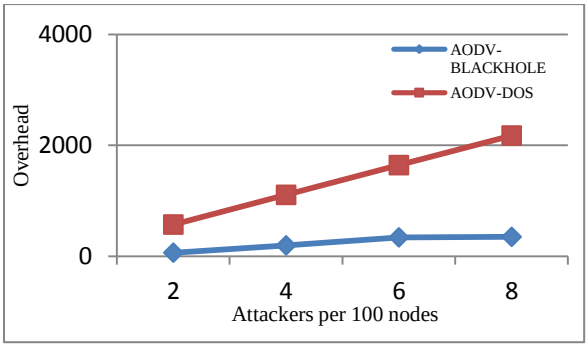

Fig.2. Overhead on DOS and Black hole Attacks vs Number of Attackers

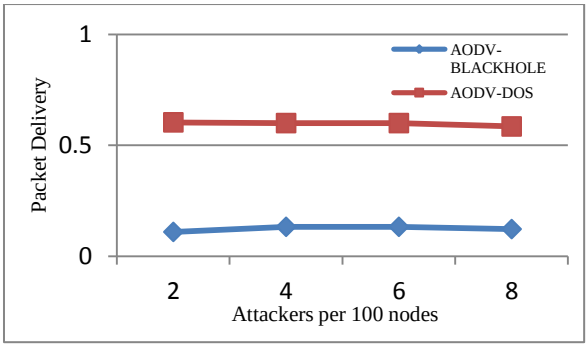

Fig.3. Packet-Delivery on DOS and Black hole Attacks vs Number of attackers

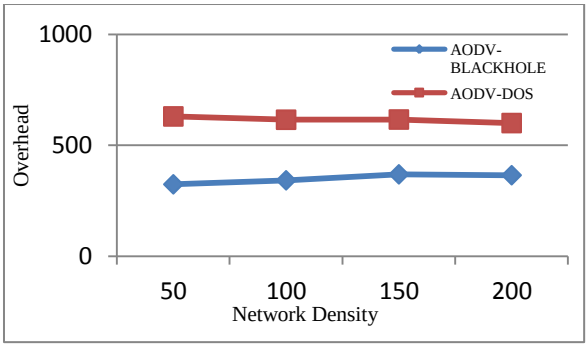

Fig.4. Overhead on DOS and Black hole Attacks vs Network Density

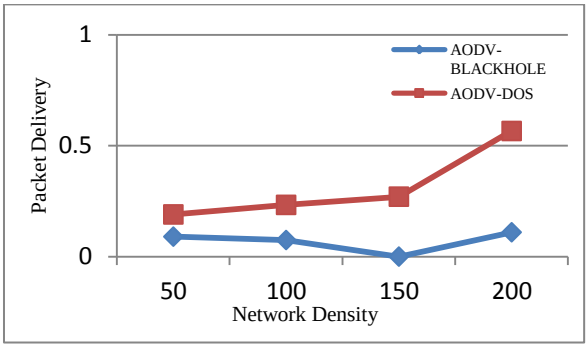

Fig.5. Packet-Delivery on DOS and Black hole Attacks vs Network Density

The Fig.2 provides the overhead in the network, when it is under black hole and DoS attacks. It can be inferred from the

result that the overhead increases linearly when the network is affected by DoS attack. DoS attack contributes more overhead compared to black hole attack. And as observed in Fig.5, black hole attack contributes for very less packet delivery compared to DoS attack as the maximum packets are absorbed by the attackers.

It can be observed from Fig.4, as the network density increases, the overhead by DoS attack decreases and overhead by black-hole attack increases , as network density increases, the scope for DoS attack reduces and the scope for black-hole attack rises. Hence in designing a common solution for Dos attach and Black hole attack ,care must be taken to optimize the overhead changes effectively.

As packet delivery increases, the network density increases, because of availability of alternative routes which may avoid the malicious route. Also, it can be inferred from Fig.3 and Fig.5, that the packet delivery performance is poorer in case of Black hole attack. Hence, while designing a solution for Black hole attack, the packet delivery needs to be addressed properly. From Fig 4, it can be clearly that with the change in network density, DoS contributes for more overhead. For designing a solution for black-hole attack, the other parameters like battery consumption, and the effect of need to be taken into consideration.

5. CONCLUSION

In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various security attacks and achieve better network performance. DoS attack contributes for more overhead and Black hole attack contributes for lesser packet delivery. In this paper the major security attacks in MANET and their effect on network performance is investigated. Hence it poses a challenge in designing an optimized solution for both the attacks.

6. ACKNOWLEDGMENTS

Above all, the authors are grateful to all our colleagues for giving us from time to time valuable suggestions , guidelines, and moral support interest of this study. We would also like to thank our family members for their co-operation for the preparation of this research paper.

7. REFERENCES

[1] Y. Xiao, X. Shen, and D.-Z. Du, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", WIRELESS/MOBILE NETWORK SECURITY, Springer 2006.

[2] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011, ISSN 2151-9617

[3] Shivanajay Marwaha, "Challenges and Recent Advances in QoS Provisioning, Signaling, Routing and MAC protocols for MANETs".

[4] Giovanni Di Crescenzo, Renwei Ge, "Securing Reliable Server Pooling in MANET Against Byzantine Adversaries", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[5] Yih-Chun Hu , Adrian Perrig , David B. Johnson "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols". *Proc. of ACM WiSe 2003.* September 2003.

[6] I. Aad, J.-P. Hubaux, and E. W. Knightly, "Denial of Service Resilience in Ad Hoc Networks",. *Proc. of ACM MobiCom '04*, 2004, pp. 202.215.

[7] Yingbin Liang , "Secrecy Throughput of MANETs Under Passive and Active Attacks", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 57, NO. 10, OCTOBER 2011.

[8] Q. Gu, P. Liu, S. Zhu, and C.-H. Chu, "Defending Against Packet Injectionin Unreliable Ad Hoc Networks".*Proc. of IEEE GLOBECOM'05*, 2005.

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

AUTHOR"S PROFILE

K.Sreenivasulu presently working as professor & HOD CSE in Madina Engineering College Kadapa.AP He is currently pursuing Ph.D from JNTUK He received B.E in Computer science from Bangalore University. He received his M.Tech in Computer Science from JNT University. He is having more than 14 years of experience in teaching. He has guided several graduate & post graduate students in their Academic projects.

Dr. E. V. Prasad received B.E. degree in ECE from S.V. University, Tirupati, A.P., India, in 1975. He obtained M.E. in Control Systems from Madras University, Madras, India, in 1978. He received his Ph.D. degree in Computer Science and Engineering, from University of Roorkee (IIT Roorkee) in 1990. He is having 34 years of teaching experience. He received best teacher award from Government of Andhra Pradesh, in the year 2008. During his teaching profession, he worked at different capacities such as Lecturer, Senior Lecturer, Assistant Professor, Professor, Head of Department of CSE, Vice Principal, Principal, Director I.S.T and Registrar JNTUK. Currently he is working as Rector J.N.T University Kakinada, Kakinada, India. He co-authored three text books. He is life member of ISTE, IE(I), CSI, and IEEE. He has more than 95 research publications in proceedings of National, International Conferences, National and International Journals.

Dr.A.Subramanyam received his Ph.D. degree in Computer Science and Engineering from JNTU College of Engineering, Anantapur. He has obtained his B.E. from University of Madras and M.Tech from Visweswaraiah Technological University. He is having 20 years experience in teaching. He is currently working as professor & HOD in the Department of Computer Science Engineering of Annamacharya Institute of Technology & Sciences, Rajampet, KADAPA Dist. A.P.. He has presented and published number of papers in international and national conferences and number of technical paper in international and national journals. He is guiding few Ph.D.s. His research areas of interest are parallel processing, image processing, network security and data ware housing, mobile computing.