2012 3rd International Conference on Information Security and Artificial Intelligence (ISAI 2012)
IPCSIT vol. 56 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V56.27

Performance of Mobile Adhoc Networks in Presence of Attacks

Konagala Pavani[1+] and Damodaram Avula[2]

[1]Department of Computer Science and Engineering, Vaagdevi College of Engineering, Jawarharlal Nehru Technological University, Hyderabad, Andhra Pradesh
[2]Director, Academic Audit Cell SE, JNTU, Hyderabad, Andhra Pradesh

Abstract. Mobile ad-hoc network is a collection of wireless mobile nodes which forms a temporary network without any fixed infrastructure or centralized administration. Mobile ad-hoc networks are widely used in the tactical battlefield, emergency search and rescue missions. They are also well used in civilian ad-hoc situations like conferences and classrooms due to the ease and speed in setting up such networks. The wireless ad-hoc networks are mostly vulnerable to security attacks because of its features like open medium, dynamic topology, lack of centralized management, node mobility, limited physical security, and limited bandwidth. In this paper we simulate black hole and gray hole attacks on Ad-hoc On Demand Distance Vector (AODV) routing protocol. Further the performance of routing protocol AODV is evaluated under these attacks by considering different metrics and scenarios. We have used network simulator 2 (ns-2) to conduct simulations on MANET. Simulation results indicate that the AODV routing protocol suffers from decreased throughput and increased packet losses in presence of black hole and gray hole attacks.

Keywords: MANET, AODV, Black hole attack, Gray hole attack, Security

1. Introduction

A mobile ad hoc network (MANET) sometimes called as mobile mesh network consists of a collection of peer mobile nodes that are capable of communicating with each other without help of a fixed infrastructure. As MANETs provide mobile nodes with reliable routing services in the absence of a network infrastructure, they are emerging as a promising platform for a variety of applications in military and civilian domains, sensor networks, rescue operations, students on campus, free internet connection sharing.

Further, MANETs are decentralized networks and the network topology is unpredictably dynamic because of node mobility. As a result, mobile nodes in MANETs act as both hosts and routers and need to discover the dynamic topology and deliver messages by themselves. These mobile nodes establish the routing tables by exchanging routing messages with each other and then deliver the data packets for others. Therefore, developing a system to maintain routing tables reliably is the most fundamental and critical issue related to MANETs.

MANETs are much more vulnerable to attacks [1] [2] than wired networks. Therefore providing security service in MANET is challenging that has attracted several researchers in this field [3, 4 and 5].

The rest of this paper is organized as follows. In section 3, we discuss the related work. Routing protocols and overview of AODV routing protocol are discussed in section 4. We present different types of attacks a MANET undergoes and description of these attacks in section 5. Section 6 and 7 presents simulation environment and results. Finally, the conclusion is in section 8.

+ Corresponding author. Tel.: + (9989041767); fax: +(0870-2865185).
E-mail address: (bandaripavani@gmail.com).

2. Related Work

As MANETs [6] are very popular, they are very much exposed to attacks. Wireless links and dynamic behavior also makes the MANET more vulnerable to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [7]. Different kinds of attacks have been analyzed in MANET and their effect on the network[2][7].The performance of the routing protocols OLSR, AODV and DSR[8][9] was examined by considering the metrics of packet delivery ratio, control traffic overhead and route length by using NS-2 simulator [10][11]. The performance of the routing protocols OLSR, AODV, DSR and TORA was also evaluated with the metrics of packet delivery ratio, end-to-end delay, media access delay and throughput by also using OPNET simulator [12][13][10].

3. Routing Protocols

The primary goal of routing protocols [14] in ad-hoc network is to establish optimal path (min hops) between source and destination. MANET routing protocols can be classified according to the protocols mechanism of route discovery and route update, into three categories: proactive (table-driven), reactive (on-demand) and hybrid.

3.1. Proactive routing protocols

In this type of protocol, the nodes try to create route in advance before there is a need to royte traffic from a specific source to destination.

Ex.DSDV (Destination Sequence Distance Vector)

3.2. Reactive routing protocols

In this type, the routes are established between two nodes only when there is a need to send actual traffic between those nodes.

Ex: Ad-hoc On-Demand Distance Vectoring [1] [15] (AODV), Dynamic Source Routing (DSR).

3.3. Hybrid routing protocols

These protocols show the characteristics of both reactive and proactive routing protocols.

Ex: Zone Routing Protocol (ZRP), ZHLS etc.

4. Types of attacks

Attacks can be classified as internal and external attacks based on the source of attacks. External attacks are done by unauthorized users and these attackers are not necessarily disconnected from the network, though. The targeted network might be a self-contained entity that is linked to other networks using the same infrastructure or communication technology .Whereas internal attacks are sourced from inside a particular network. A compromised node with access to all other nodes within its range poses a high threat to the functional efficiency of the whole network.

Another type of classification is active attack and passive attack. Some attacks are classified according to the layer of occurrence are discussed below. In this paper we have implemented black hole and gray hole attacks which occurs in network layer using AODV routing protocol.

4.1. Black Hole Attack

Black hole attack is an active attack type, which leads to dropping of messages.In this type of attack, malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives a RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself. This black hole node assigns a high sequence number to settle in the routing table of the victim node and sends before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over the malicious node. In the same manner the malicious node attacks all RREQ messages and takes over all routes. Therefore all packets are sent to black hole node. The black hole node without forwarding the packets to the destination

discards them. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network. In this way a black hole node can affects the whole network.

4.2. Gray Hole Attack

The AODV routing protocol is vulnerable to gray hole attack. It is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward the packets and then fails to do so. Initially the attacker node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets. If neighboring nodes (that try to send packets over attacking nodes) lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption).

5. Simulation Environment

Simulations are often used to model natural, machine or human systems in order to gain insight into their functioning. Network Simulator ns-2 [18] [19] is used to carry MANET simulations.NS-2 is a simulation project developed by the University of California Berkley. NS is part of software of VINT [20] project which is supported by DARPA since 1995. It is one of the most widely used network simulators for wired and wireless networks. NS2 is an object–oriented, discrete event driven network simulator which is written in C++, with an OTcl interpreter as a frontend, and is available free. It follows the layered approach, and is accompanied by a rich set of protocols.

We run two simulations, one without the attacker node and other including the attacker node. we have repeated the experiments by changing the number of nodes to 40,60 and 80 to see the performance of network under attacks. The simulation parameters are shown in table 1

Table. 1: Simulation Parameters

Parameter	Definition		Parameter	Definition
Protocol	AODV		Simulation Area	1000*1000
Mac Layer	IEEE 802.11		Size of data Packet	512
Simulation Time	500s		Traffic sources	CBR
Connection Time	450s		Number of nodes	20,40,60,80
Node Placement	Random		Version NS2	NS-2.29(under windows,cygwin)
----------	--------		Data rate	10kbits

6. Experimental Results

Figure 1 shows the designed network with 20 nodes in which one node is a black hole node. Figure 2 shows the designed network with one grayhole attack node. A simulation study was carried out to evaluate the performance of MANET in presence of attacks using metrics such as throughput, packet losses and packet delivery ratio.

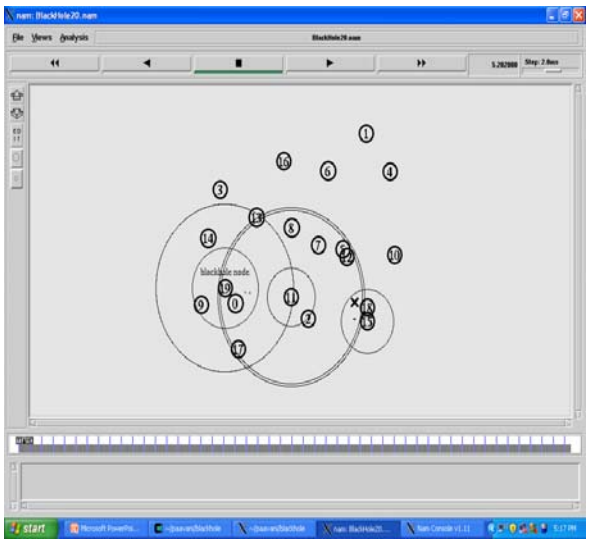

Fig. 1: Network with blackhole attack

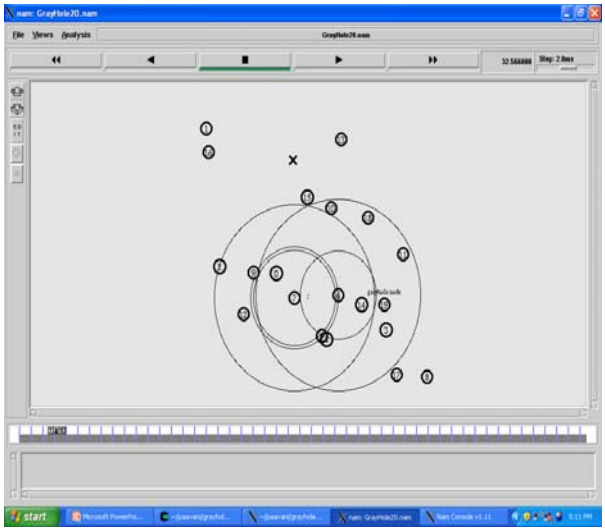

Fig. 2: Network with grayhole attack node

7.1. Throughput

It is the amount of data transferred from sender to receiver in a given amount of time. It is measured in bits per sec or packets per sec. Throughput is calculated for the network in normal condition and then in presence of attacks. Throughput values for 20 nodes are calculated at pause times 20s,40s,60s,80s.These values are listed in Table 2 and they are plotted in graph as shown in figure 3.Based on simulation results we can analyze that , the throughput of network under black hole and gray hole attacks decreases when compared to the network under normal conditions.

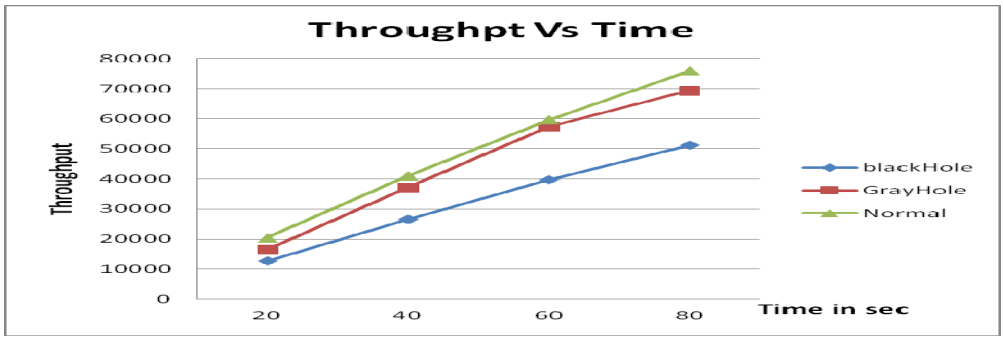

Fig. 3: Comparison of Node Throughput for 20 nodes

Table. 2: Throughput Values for 20 nodes

Pause time in secs	Blackhole	Grayhole	Normal
20	12654	16379	20336
40	26478	37147	40885
60	39706	57448	59613
80	51260	69415	75867

7.2. Packet Loss

Number of packet loss can be calculated by subtracting the received packets from send packets. These values are calculated for different scenarios like 20, 40, 60 and 80.These values are listed in Table 3 and plotted as shown in the figure 4. Based on simulation results, we observe that the packet loss of network under normal condition is less than that of network under black hole and gray hole attacks.

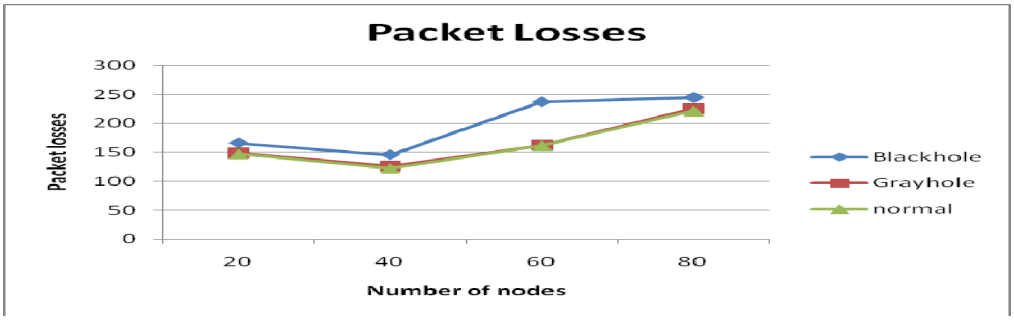

Fig. 4: Impact of attacks on packet loss

Table. 3: Packet loss for different scenarios

Nodes	Blackhole	Grayhole	Normal		Nodes	Blackhole	Grayhole	Normal
20	166.01	148.70	147		60	236.75	162.14	161.50
40	145.68	125.6	122.00		80	244.44	225.09	221.30

7.3. Packet Delivery Ratio

It is the ratio of data packets received by the destination to those sent by the source. It is calculated by dividing the number of packet received through the number packet sent from source. Packet Delivery Ratio (PDR) is calculated by considering number of nodes as 20, 40, 60 and 80.These values are listed in Table 4 and they are plotted in graph as shown in figure 5.PDR characterizes both correctness and efficiency of network. A high PDR is desired in any network. It is observed from the simulation that PDR value of network in normal condition is higher than the network under attacks.

Table. 4: PDR values for different scenarios

Number of nodes	Normal	Blackhole	Grayhole		Number of nodes	Normal	Blackhole	Grayhole
20	86.57	8.05	85.75		60	97.79	0.59	89.63
40	98.63	1.70	87.96		80	97.07	1.83	82.63

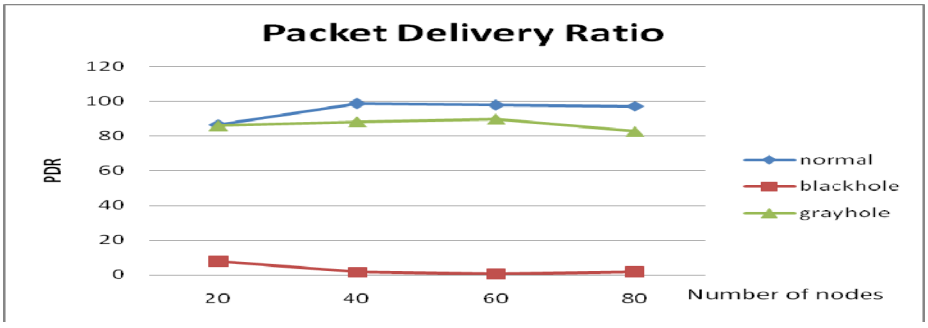

Fig. 5: Impact of attacks on PDR

7. Conclusion

The security of the Ad Hoc network routing protocols is still an open problem and deserves more research work. In this paper, we have analyzed the security threats faced in an ad hoc network. We have implemented Black hole Attack and Gray hole Attack against AODV routing protocol using Network Simulator-2.we have analyzed the performance of network under these attacks by considering different performance metrics. This research defines a first fruitful effort towards the definition of an attack

implementation for auditing the resilience of Ad Hoc routing protocols and discovering new vulnerabilities in such communication elements.

8. References

[1] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, Abbas Jamalipour. A survey of routing attacks in mobile ad hoc networks, *IEEE Wireless Communication*, 14 (5), pp. 85-91,2007

[2] K. Biswas and Md. Liaqat Ali, Security threats in mobile ad-hoc network, *Master Thesis*, Blekinge Institute of Technology Sweden, 22nd March 2007.

[3] Y. Zhang, W. Lee, and Y. Huang, Intrusion detection techniques for mobile wireless networks, *Wireless Networks, v*ol. 9 no. 5, pp. 545-556., 2003.

[4] D. E. Denning, An intrusion-detection model, *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222-232, February 1987.

[5] J. P. Anderson, Computer Security Threat Monitoring and Surveillance. Fort Washington: James P. Anderson Co., 1980.

[6] Y. Zhang and W. Lee, Intrusion detection in wireless ad hoc networks, *Mobicom 2000*

[7] P.V.Jani, Security within ad-hoc networks, Position Paper, *PAMPAS* Workshop, Sept. 16/17 2002.

[8] Mohammed Bouhorma, H.Bentaouit and A.Boudhir, Performance comparison of ad hoc routing protocols aodv and dsr",*IEEE*,2009.

[9] Wang Lin-zhu, FANG Ya-qin and SHAN Min, Performance comparison of two routing protocols for ad hoc networks, *WASE International conference on Information Engineering*,2009.

[10] P. Manickam, T. Guru Baskar, M.Girija, Dr.D.Manimegalai, performance comparisons of routing protocols in mobile adhoc networks, *International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1, February 2011*.

[11] Saiful Azadm, Arafatur Rahman and Farhat Anwar, "A Performance comparison of Proactive and Reactive routing protocols of Mobile Ad hoc Networks(MANET)", *Journal of Engineering and Applied Sciences*, 2007.

[12] Nadia Qasim, Fatin Said and Hamid Aghvami, Mobile ad hoc networks simulations using routing protocols for performance comparisons, *Proceedings of the world congress on Engineering*, WCE, VOL I, 2008.

[13] C.Mbarushimana and A.Shahrabi, Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks, *AINAW-IEEE*, 2007.

[14] Elizabeth M. Royer et. al. A review of current routing protocols for ad hoc mobile wireless networks, *IEEE Personal Communication*, April 1999.

[15] C. Perkins and E. Royer. Ad-hoc on-demand distance vector routing. In the 2nd IEEE workshop on *Mobile Computing Systems and Applications*, February 1999.

[16] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong A new routing attack in mobile ad hoc networks,In the I*nternational Journal of Information Technology* Vol. 11 No. 2.

[17] R.H. Khokhar, Md. A.Ngadi, S. Manda. A review of current routing attacks in mobile ad hoc networks, International. *Journal of Computer Science and Security*, 2 (3), pp. 18-29, 2008.

[18] http://www.isi.edu/nsnam/ns/ K. Fall and e Varadhan. The ns Manual (formerly ns Notes and Documentation), 2000.

[19] NS by example http://nile.wpi.edu/NS/overview.html,14 May 2006.

[20] Virtual IntercNetwork Testbed, http://www.isi.edu/nsnam/vint, 14 May 2006.

Pavani Konagala, Associate Professor at Vaagdevi College of Engineering, Bollikunta, Warangal. She has completed B. Tech from Kakatiya Institute of Technological Sciences, Warangal and M. Tech from Jawaharlal Nehru Technological University, Hyderabad. She has 8 years of experience and has performed as project co ordinator, Co ordinator for technical symposium and guided B. Tech and M. Tech students for their dissertation projects. She is a prime member of various committees in the department for organizing events in the college. She is presently pursuing her Ph. D from JNTU

Hyderabad and presented papers in few conferences and she has one publication to her credit.

Dr. Avula Damodaram was recipient of DISTINGUISHED ACADAMICIAN AWARD by Pentagram Research Centre, India, in January 2010. Dr Damodaram has more than two decades of dedicated service in Department of Computer Science & Engineering and performed distinguished services to the University as a Professor, Head of the Department, Vice Principal, Director of UGC-Academic Staff College, Director, School of Continuing & Distance Education and Director, University Academic Audit Cell. He has successfully guided 10 Ph.D. scholars and currently guiding 9 scholars for Ph. D. Dr. Damodaram is on the editorial board of 2 International Journals and a number of Course materials. Dr Damodaram successfully executed an AICTE research project at a cost of 7 Lakhs. He has been a UGC nominee for a number of expert and advisory committees of various Indian Universities. Dr. Damodaram has published 45 well researched papers in national and International journals. He has also presented 59 papers at different National and International conferences at United States of America, Austria and the United Kingdom etc.