Performance Analysis of MANET Under Grayhole Attack Using AODV Protocol

Samiran Gupta and Harsh Nath Jha

Abstract Mobile ad hoc network (MANET) has been a challenging field with its foremost criteria like heterogeneity of nodes, dynamic topology, energy constraint and security over the years. MANETs are globally popular for their cost-effectiveness ease of access and configuration. However, MANETs are vulnerable to many types of attacks like Blackhole, Wormhole, Grayhole, etc., which makes MANETs pretty much risky to rely upon when scaling up on a large scale. Under mobile ad hoc networks, all the transmission between the mobile nodes occurs wirelessly. Due to the infrastructure-less, self-organizing and dynamic nature of the nodes, it is an arduous task to enforce any security solutions against these kinds of vulnerabilities. Ad hoc on-demand vector (AODV), a supremely significant route-on-demand routing protocol for MANET, relies on the routing table at each intermediate node location. In this paper, we are mainly analyzing the performance of a MANET under Grayhole attack as per AODV routing protocol using NS-2 simulation environment.

Keywords Mobile ad hoc network · Grayhole attack · Wireless networks · Ad hoc on-demand vector · Smart node · Dynamic routing protocols · Throughput · Quality of service

S. Gupta (✉)
Department of Computer Science and Engineering, Asansol Engineering College, Asansol, West Bengal 713305, India
e-mail: samiran.bappa@gmail.com

H. N. Jha
Department of Information Technology, Asansol Engineering College, Asansol, West Bengal 713305, India
e-mail: ind.harshit@gmail.com

S. K. Das et al. (eds.), *Architectural Wireless Networks Solutions and Security Issues*, Lecture Notes in Networks and Systems 196,
https://doi.org/10.1007/978-981-16-0386-0_15

1 Introduction

Mobile ad hoc network (MANET) [1] is constituted of dynamically self-orienting mobile nodes, making it an infrastructure-less model of network design. These nodes may function as servers as well as clients, as required, demolishing the demand of a dedicated server or router in the network [2]. This provides autonomity to the system, boosting its performance. These nodes have the ability to create a suitable path for the communication channel to form and function. However, MANETs are not a good choice if seen from the point of view of security and integrity of data. The absence of a dedicated server or router may also produce serious security breaches as there is nearly no authentication or encryption available.

MANET as a network arrangement is also much cost effective than the conventional ones, although they cannot be scaled up to a large scale, as despite having undeniably excellent features, have never been a preferable choice as the data in the communication channels are left exposed to tons of security threats and other limitations that are associated with MANETs.

Figure 1 presents a pictorial portrayal of the arrangement of the nodes in the network and their configuration to form a bigger communication channel. We have a total of 7 nodes participating in the channel with no dedicated router or a similar central medium to act as a bridge to connect the nodes. The individual nodes have one or more transceivers between them [3]. The application of MANETs is not as popular in small or medium-sized business or personal/home networks, as compared to a conventional router-driven setup.

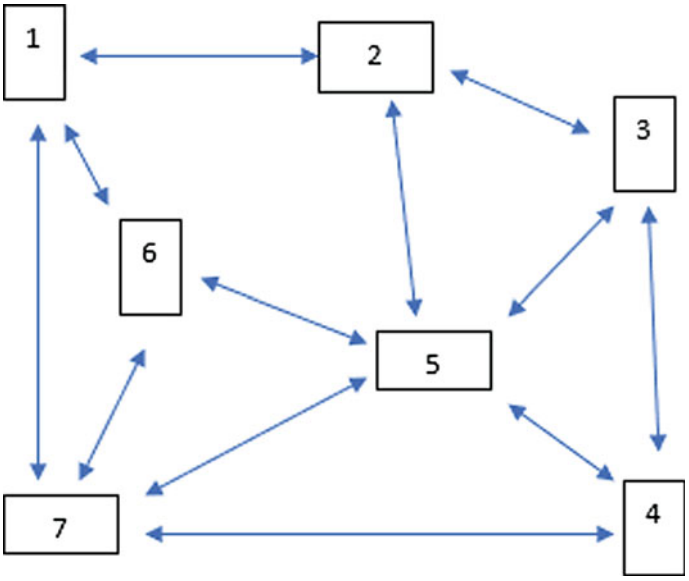

Fig. 1 Overview of MANET

Although MANETs have tons of advantages to count on [4], the flip side of the coin has some serious demerits of MANETs, which are mostly security oriented. These types of networks are mostly prone to Grayhole attack, especially when operating under the AODV protocol.

2 Literature Study

We are presenting an elaborative study on MANET and its characteristics (Sect. 3), its overview (Sect. 3.1) and its working principle and the AODV routing protocol (Sect. 3.2). In Sect. 4, we have presented the problem statement, i.e., about the risks that MANETs are exposed to. Section 5 gives an account on Grayhole attacks and its functional mechanism. For generating a real-like attack on a dummy network arrangement have used NS-2 (network simulation environment), via Linux Fedora. We have discussed the attack environment in Sect. 6, while Sect. 7 contains results and comprehension of our simulation.

We have tried to stress on the risks that MANETs come packaged with, which will facilitate us and also other researchers to come up with better solutions against this kind of attacks and be able to fix those issues, resulting in making MANET a safer communication environment than before.

In this section, we discuss some related and underlying research works by different researchers/authors in the field of wireless networks and Grayhole attacks. Over time, a considerable number of researchers have shared their ideas, findings and conclusions in this subject and also suggested several defense techniques to detect and diffuse Grayhole attacks on ad hoc networks based on intrusion detection systems (IDS) and related mechanisms.

Gupta [5] et al. discuss about sensor networks with regards to load-based routing schemes. Through their work on MANET, Jha et al. [6] shed light on the loss of performance and other security breaches associated with Wormhole attacks. Many authors have worked on Grayhole being launched on ad hoc wireless networks, which itself highlights its severity. Sharma [7] has done a survey on Grayhole attacks on MANETs, which makes it crystal clear that Grayhole attacks can prove deadly in terms of compromising with the network. Dhaka et al. [8] proposed a method to detect Grayhole attacks and Blackhole attacks in MANETs. Later on, Aarti et al. [9] and Mittal [10] have proposed an enhanced multipath approach to deal with the threat of Grayhole attacks on MANETs.

Researchers in this field have made noteworthy breakthrough in this area, but unfortunately, we are yet to have a high-accuracy defense system against Grayhole attack. With regards to the scope for development that we have in this area, we are properly visualizing the attack scenario in a detailed fashion through this paper for (we researchers) being able to develop an enhanced fighting mechanism against Grayhole attacks.

3 Brief Study of Mobile Ad hoc Networks:

i. Dynamic topology: MANET's multi-hop network topology is capable of sudden and spontaneous reorganization in both unidirectional and bi-directional routing architecture.
ii. Cost effective: Being hardware-less and peer-to-peer in nature, MANETs are considerably cheaper for small to medium level business as well as residential networks.
iii. Power supply constraint: Battery led (or similar energy source) power supply being incorporated here is not a reliable or promising source of power per se, and it is the reason why the mobile nodes in the network have light weighted features, low power and storage capacity.
iv. Autonomous/self-configuring: The prime feature of MANETs is the ability of its components (participating nodes) to re-role themselves into routers and hosts themselves.
v. Mediocre throughout: As MANET is a wireless form network arrangement, it struggles against factors like noise, multi-access, interference condition, etc., which dramatically reduces its productivity based on efficiency, throughput and reliability.
vi. Lack of data security: Being infrastructure-less by design, MANETs have no dedicated routers, because of which a standard host configuration or firewall rule-set cannot be enforced. This gives rise to potential threat to the data present in the channel [11] as well as the quality of service (QoS) [12] of the network.

3.1 MANET—Highlights

Wireless ad hoc networks are fairly popular with its users at a mass level. Being a 'plug and play' kind of network setup, MANETs do not require a dedicated router. Although MANET is an awesome mode of network, but it also has some flaws attached with it when implemented at a large scale. Below are some of the forward most ins and outs of MANETs:

i. Infrastructure-less mode of design.
ii. No central administration.
iii. Human intervention independent, as each node can re-purpose themselves as a router or host as needed.
iv. Vulnerable to security threats.
v. Intercommunication interferences causes poor throughput.
vi. Cost effective.

3.2 MANET—Working Principle

MANETs are mostly developed using a table-driven network protocol. AODV protocol [13] is one of the foremost protocols in this matter which enables its nodes to be follow a dynamic, self-configuring and multi-hop routing method. This proves to be a key element in route maintenance. Maintaining routes with inactive nodes are not required because of the dynamic re-routing in AODV.

If there are 5 nodes in a channel and only three of them are participating in an active communication and the remaining two are merely present in the network, then the working nodes need not preserve a route with them. To promote optimal load balancing, AODV supports real-time re-routing and re-orientation of the nodes and avoid any disruption in the channel.

Each node has a specific range till which it can establish communication. This is much similar to a scenario of a classroom where a student from the first bench wants to pass a notebook to their friend at the last bench. Here, the notebook will be passed to the recipient student via many students acting as intermediate sender. If the destination node in MANET is unreachable from the sender, then the nodes use a similar strategy of sending it via multiple intermediate senders. This process is known as multi-hopping in AODV routing premises.

These nodes are designed to be able to re-design the network topology as a response to a security breach, when detected. Once a malicious activity is reported in any node, it is denied permission to perform any action in the communication channel. Again, since this whole process may require some time and until then some sensitive data might already have been compromised; hence, it cannot be accepted as a fail-safe mechanism.

AODV strictly follows a request-reply technique to verify the authenticity of the participants in the network. It contains a few message type definitions such as route requests (RREQs), route replies (RREPs), route errors (RERRs) and acknowledgment (ACK). For every transfer of a data packet, the source generates a route request (RREQs) toward the recipient node and the receiving node replies with an acknowledgment (ACK) of receiving the data in order to prove its authenticity. In case if this process fails, a breach is assumed to have taken place and it leads to broadcasting an error message (RERRs), which immediately suspends all transactions until the node is verified.

AODV routing involves of a couple of episodes:

i. Discovery: Discover new paths using RREQ and RREP.
ii. Maintenance: Report an error when found, using RERR.

AODV protocol maintains a separate routing table per node. Each node's route table contains information about the distance to other nodes in the channel, which is measured in terms of hop-counts. The route table contains the following details gathered while the route discovery phase:

i. Source/previous node
ii. Next node/hop
iii. Time to leave (TTL)
iv. Hop-count to reach destination
vii. Destination IP address.

4 Problem Statement

MANET has many challenges when scaling out on large scale, but it becomes worth a little more concern from the security hotspot as it is vulnerable a plethora of attacks [14, 15]:

i. Session hijacking [16]
ii. Wormhole attack [17]
iii. Blackhole attack [18]
iv. Jamming [19]
v. Eavesdropping [20]
vi. Denial of service [21]
vii. Grayhole attack [22].

Grayhole attack is one of the deadliest attacks against MANETs with regards to:

i. Throughput: The ability of the network to transfer a particular quantity of information per unit time is known as throughput. In other terms, it is the measure of a network's efficiency.
ii. Quality of service (QoS): It is the maximum bandwidth attaining capacity of a network, which affects other parameters such as latency, error rate and uptime [23]. Thus, higher QoS translates to a healthier performance.
iii. Data rate: Also knows as data transfer rate, it is the measure of the number of bits of data transmitted per second over a network. In simpler terms, it is the speed of data transfer over the network, conveyed as bytes per second (Bps or B/s)
iv. Integrity: It enforces that a dataset MUST only be accessed by an authorized and intended user, i.e., if a data is not meant for a particular entity, it must be forbidden for them and it should be private to the legitimate user only [24].

For the sake of analyzing the effects of Grayhole attack on the performance of MANET, we are simulating a dummy network with a number of nodes against a Grayhole attack scenario using AODV routing protocol.

5 Grayhole Attack

Grayhole attack [25, 26] is basically a packet drop attack, which is an extension of Blackhole attack. Here, the routing packets and control are forwarded by the malicious or Grayhole node, but the data packets are completely dropped. This attack uses the method of selective data packet dropping to disguise the compromised node as a legitimate one. This node tries to take part in the data transfer window, and then by advertising a false route, it lures the legitimate nodes to establish the active route through itself. The Grayhole node responds with a route reply after receiving a route request packet and thereby passes a false information that of having the shortest path, which creates an illusion for the source node that the optimum route is through the malicious node and the data packets are redirected toward the malicious node. This series of incidents gives rise to a confusion in the detection and prevention mechanism as packets may as well sometimes drop due to genuine reasons like: congestion, overload, etc. The following are the two ways how Grayhole attacks work:

i. Strictly dropping all the incoming UDP packets.
ii. Randomly/selectively dropping some UDP packets.

Due to its ability to act both as a normal node and switch over to malicious node as needed, a Grayhole node changes its behavior from a legitimate node to a sinkhole, which fools the system to identify whether it is indeed a genuine node or a compromised one. The Grayhole attack takes place in two phases, as below:

i. In this stage, the malicious node exploits the AODV routing protocol table by diverting all the data packets to itself rather than genuine route; thus claiming itself as the shortest route in next hop column.
ii. The attack is launched in this phase where malicious node starts dropping the data packets using a probabilistic method for packet selection. The attacker node changes its behavior rapidly and the malicious node also forward some packets to create an illusion of legitimacy. Hence, this type of attack is pretty difficult to detect.

6 Simulation Environment

For the purpose of simulation, we are using Network Simulator 2 (NS-2) on a Linux Fedora distribution, which is quite a familiar and popular simulator in MANET research community due to its ease of access and because it supports a variety of network routing protocols. NS-2 is an object-oriented network simulator written using C++ as its backend and object Tcl (OTcl) as its front-end and runs on top of UNIX environment. Below are the details of our attack environment and the parameters at which the system was tuned in to (see Table 1).

Initially, the network is simulated under normal and stable conditions, i.e., without any attack and its throughput is recorded. Later on, we generated an attack of Grayhole

Table 1 Configuration details of the simulation environment

Parameter	Value/type
Number of mobile nodes	10
Link layer type	LL
Antenna type	Omni antenna
Simulation duration	1200 s
Propagation model	Two-way ground
Mobility model	Random waypoint
Interface type	Phy/WirelessPhy
MAC type	Mac/802.11
Interface queue type	Queue/DropTail/PriQueue
Routing protocol	AODV
Channel type	Wireless channel
Simulation area	1000 m × 850 m

nature on the same setup to record and analyze its throughput in order to be able to comprehend the aftermaths of the attack on the network. Here, we noticed that the network throughput drops to zero immediately as soon as the channel in under the attack (Fig. 2).

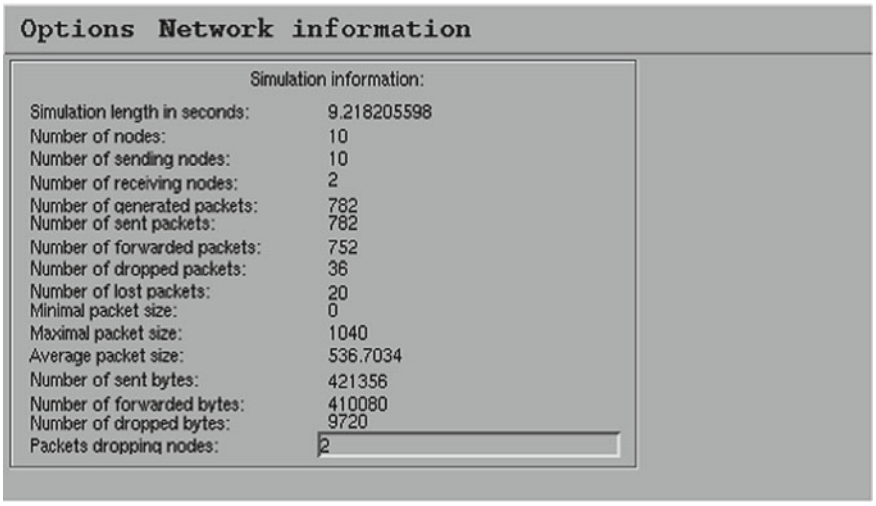

Fig. 2 Simulation information of our dummy network

Throughput: The average amount of data transferred between the sender and receiver nodes per unit time within a network is called throughput. It is expressed in terms of kilobytes per second (kbps) and calculated using the following equation (see Eq. 1).

$$\text{Throughput} = \frac{\text{Data transferred (in bytes)}* 8}{\text{Time taken (in seconds)}} \quad (1)$$

7 Attack Simulation and Results

Scenario 1: Without Attack

I. Deploying the mobile of nodes

As shown in Fig. 1, we started deploying nodes to participate in the network. There are no dedicated routers or a similar central administration device present in the network (Fig. 3).

II. A self-arranged ad hoc networks by the deployed nodes

Now as we have deployed a total of 10 nodes in the network (Fig. 4), namely 0 till 9, we observe the nodes interacting with each other as per the AODV protocol.

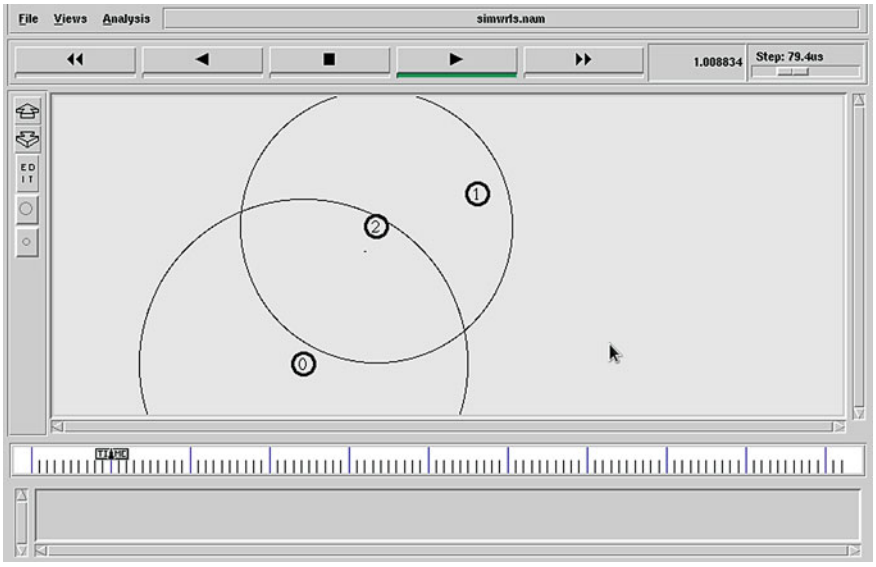

Fig. 3 Deploying the nodes

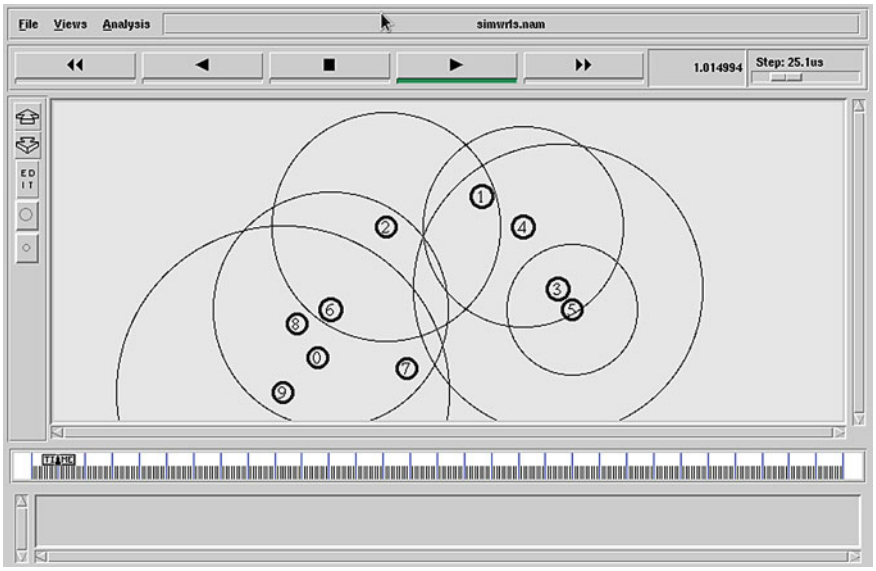

Fig. 4 Individual nodes forming an ad hoc network

III. Identifying the source, destination and forwarder nodes

MANETs are dynamic and self-organizing in nature, i.e., it decides the communication path, thus as seen in Fig. 5, we have a source, a destination and an intermediate node to facilitate the communication as the source and destination are not reachable to each other directly. Whenever there is a scenario like this where the source and destination nodes are unreachable (as their reachable zone is limited), MANETs adapt a multi-hop mechanism to transfer data.

IV. Communication via the established path

In the previous step, we already had our source, node and intermediate nodes identified. In this step, we can actually see the data transfer in action (Fig. 6). There is no loss of data and the communication is happening smoothly. This is an ideal case, without any attack, characterized by a stable throughput and QoS.

Scenario 2: Network under attack

V. Malicious node starts dropping packets

Until now, we were simulating the best case for data transfer with optimum throughput. At this point of time, we launched a Grayhole attack on the network with node '2' dropping the data packets. It is pretty obvious from Fig. 7 that the communication is still happening but the data rate is considerably lower than before, as a lot of data is being drained by the malicious node.

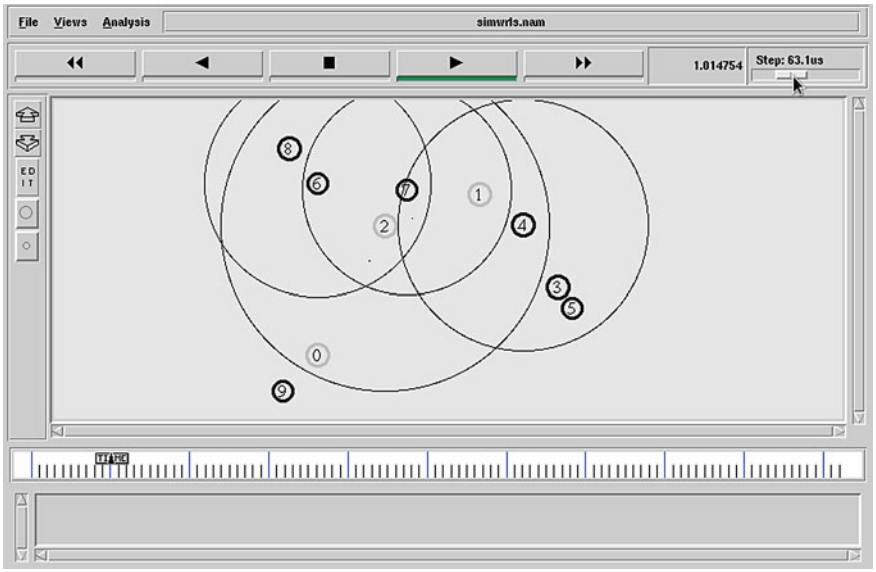

Fig. 5 Identifying sender, receiver and intermediate nodes

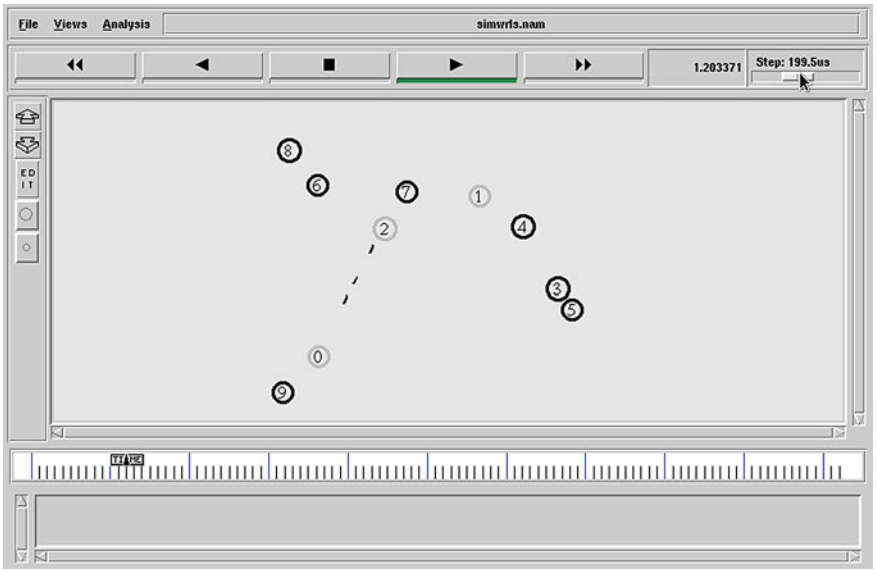

Fig. 6 Data transfer under normal circumstances

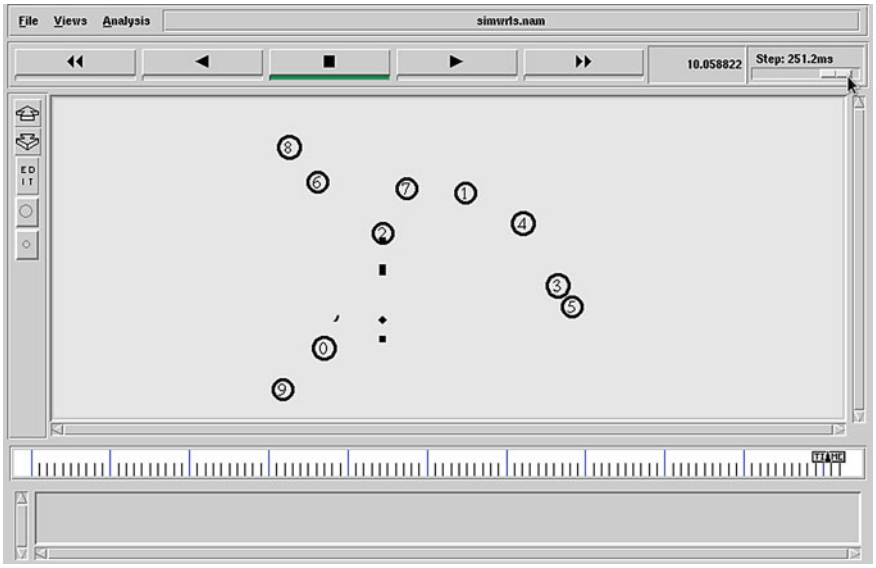

Fig. 7 Malicious node starts dropping data

VI. Loss in throughput

Evident from Fig. 8, we can confirm what we saw in the previous step. The channel's throughput spikes fall miserably, and at the same moment, we launched attack and that continued until the attack persisted.

VII. Trace file of the network scenario at the moment

Figure 9 shows the network trace of the above attack simulation of MANET. From the simulation presented above, it is clear as a mirror that Grayhole attack is indeed a prominent vulnerability to MANETs. These kinds of attacks not only put the data integrity at stake because of the possible leakage in the communication channel, but also pose great threat to the network as a whole, in terms of overall productivity.

8 Conclusion

After a detailed analysis of the performance of MANETs under the effects of a Grayhole attack using AODV protocol via NS-2 simulator, our final inference is that these kinds of ad hoc networks have a strictly linear throughput trend which starts deteriorating dramatically under an attack. Along with throughput, other factors like data rate, QoS, etc., parameters of the network were also affected at an alarming level to be considered as abnormal and concerning. The data transfer within the network kept on falling as long as the attack was kept alive on the network.

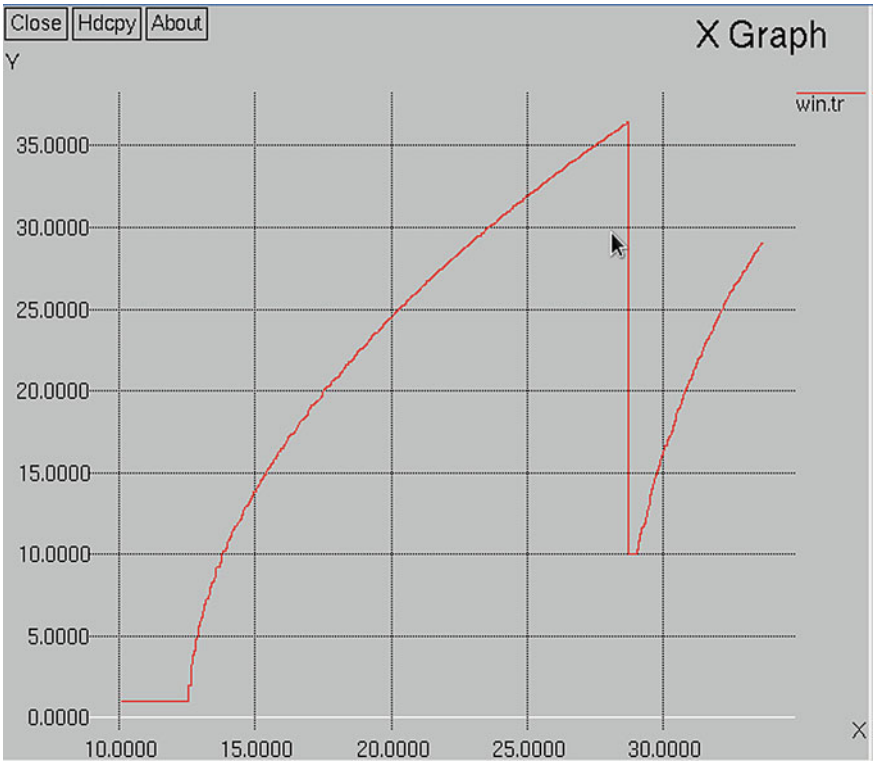

Fig. 8 Network throughput during attack

From the above analysis, it is clearly understandable how a Grayhole attack cannot only hamper the network QoS and throughput, but bully privacy as well. Grayhole attacks are difficult to detect also because the data rate does not drop to zero at once, i.e., the communication keeps on taking place, but it degrades slowly and steadily which also might be misunderstood as a usual network glitch such as channel noise or interference. Until one smells anything fishy, a lot of data might already have been leaked. However, with further advancements in the MANET's immune system and an improved intrusion detection system, it can be guarded against Grayhole attacks.

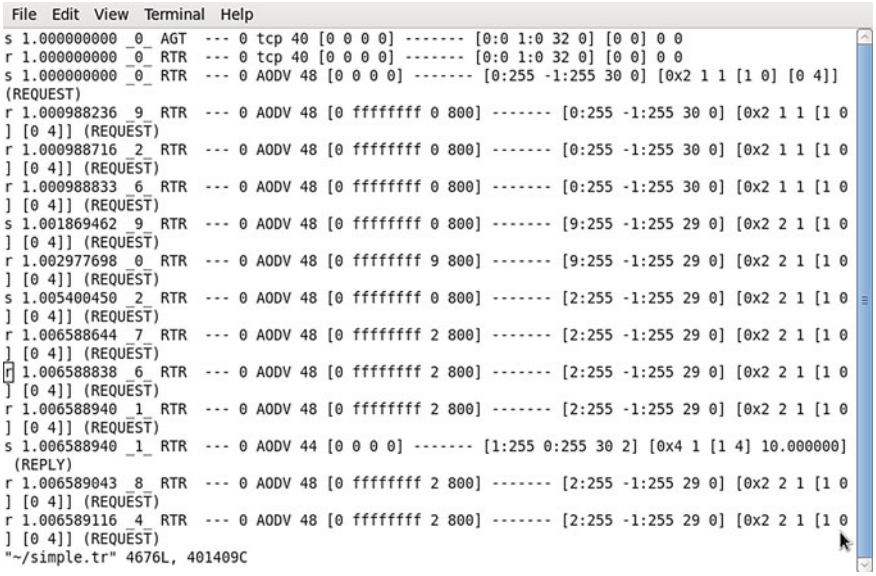

Fig. 9 Network trace while the attack

References

1. Aarti SST (2013) Study of MANET: characteristics, challenges, application and security attacks. Int J Adv Res Comput Sci Softw Eng 3(5)
2. Ali H, Shahzad W, Khan FA (2012) Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization. Appl Soft Comput 12(7):1913–1928
3. Cho J-H, Chen R, Chan KS (2016) Trust threshold based public key management in mobile ad hoc networks. Ad Hoc Netw 44:58–75
4. Das SK, Tripathi S (2018) Intelligent energy-aware efficient routing for MANET. Wirel Netw 24(4):1139–1159. https://doi.org/10.1007/s11276-016-1388-7
5. Gupta S, Das B (2013) Load based reliable routing in multi-sink sensor networks. Res Inventy Int J Eng Sci 2(12):59–64
6. Jha HN, Gupta S, Maity D (2020) Effect of wormhole attacks on MANET. In: Design frameworks for wireless networks. Springer, Singapore. https://doi.org/10.1007/978-981-13-9574-1_8
7. Sharma R (2016) Int J Comput Sci Inf Technol 7(3):1457–1460 (IJCSIT)
8. Dhaka A, Nandal A, Dhaka RS (2015) Gray and black hole attack identification using control packets in MANETs. Procedia Comput Sci 54:83–91. ISSN 1877–0509
9. Aarti PR (2015) Prevention and elimination of gray hole attack in mobile ad-hoc networks by enhanced multipath approach. Int J Eng Trends Technol (IJETT) 23(5):224–229. ISSN:2231–5381
10. Mittal V (2015) Prevention and elimination of gray hole attack in mobile ad-hoc networks by enhanced multipath approach. Int J Adv Res Comput Eng Technol (IJARCET) 4(5)
11. Yang H, Luo H, Ye F, Lu S, Zhang L (2004) Security in mobile ad hoc networks: challenges and solutions. UCLA Previously Published Works
12. Castellanos WE, Guerri JC, Arce P (2015) A QoS-aware routing protocol with adaptive feedback scheme for video streaming for mobile networks. Comput Commun 77:10–25

13. Perkins CE, Royer EM (1999) Ad-hoc on-demand distance vector routing. In: Proceedings of the 2nd IEEE workshop on mobile computing systems and applications, pp 90–100
14. Sheikh R, Chande MS, Mishra DK (2010) Security issues in MANET: a review. IEEE
15. Goyal P, Parmar V, Rishi R (2011) MANET: vulnerabilities, challenges, attacks, application. IJCEM Int J Comput Eng Manage 11:32–37
16. Lupu TG, Rudas I, Demiralp M, Mastorakis N (2009) Main types of attacks in wireless sensor networks. In: WSEAS international conference. Proceedings. Recent advances in computer engineering
17. Maheshwari R, Gao J, Das SR (2007) Detecting wormhole attacks in wireless networks using connectivity information. In: IEEE INFOCOM 2007–26th IEEE international conference on computer communications, pp 107–115
18. John NP, Thomas A (2012) Prevention and detection of black hole attack in AODV based mobile ad-hoc networks—a review. Int J Sci Res Publ 2(9)
19. Xu W, Trappe W, Zhang Y, Wood T (2005) The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of the 6th ACM international symposium on mobile ad hoc networking and computing, pp 46–57
20. Dai HN, Wang Q, Li D, Wong RC (2013) On Eavesdropping attacks in wireless networks with directional antennas. Int J Distrib Sens Netw 9(8):760834
21. Jhaveri RH, Patel SJ, Jinwala DC (2012) DoS attacks in mobile ad hoc networks: a survey. In: 2nd international conference on advance computing and communication technologies, pp 535–541
22. Sen B, Sharma K, Ghose MK, Sharma A (2015) Gray hole attack in manets. Int J Adv Electron Comput Sci 2(10). ISSN: 2393–2835
23. Basarkod PI, Manvi SS (2015) Mobility and QoS aware routing in mobile ad hoc networks. Comput Electr Eng 48:86–99
24. Ning P, Sun K (2005) How to misuse AODV: a case study of Insider attacks against mobile ad-hoc routing protocols. Ad Hoc Netw 3(6):795–819
25. Nguyen HL, Nguyen UT (2008) A study of different types of attacks on multicast in mobile ad hoc networks. J Ad Hoc Netw 6:32–46
26. Deng H, Li W, Agrawal DP (2002) Routing security in wireless Ad Hoc networks. IEEE Commun Mag 40(10):70–75