Simulation of Security Attacks and Preventions on AODV Protocol in NS-3

Alaa Hassan[1], Milena Radenkovic[2]
[1]Computer Science Department, School of Science
University of Kirkuk, Kirkuk
Iraq
[2]School of Computer Science and IT, University of Nottingham
United Kingdom
alaa.mustafa.hassan@gmail.com, milena.radenkovic@nottingham.ac.uk

ABSTRACT: *MANETs are open and cooperative networks and can be formed quickly and without any complex infrastructure. These are very useful characteristics for fast and easy connectivity, however this poses severe security threats. In this paper, we only focus on the security threats posed to most popular MANET routing protocol AODV by black hole and flooding attacks. A Simulation study has been conducted in ns-3 to compare the performance of preventive schemes FAP and AMTT in case of flooding and black hole attacks on MANET's. The performance is analyzed based on throughput, message delay and routing overhead.*

Keywords: Component, MANET, AODV, DOS, Black Hole, AMTT, FAP, NS-3

Received: 10 October 2014, Revised 24 November 2014, Accepted 30 November 2014

1. Introduction

MANETs (Mobile Ad Hoc Networks) are self-organized networks and have applications in industrial, academic and military domains. Routing in MANETs is complex and varies as compared to fixed-wire and infrastructure based Wireless networks. MANET routing have to cope up with constrained resources and infrastructure-less topologies. AODV (Ad hoc On-Demand Distance Vector) [1] routing protocol is one such protocol which is very popular in MANETs because of its lightweight stack and support for low overhead routing. MANETs routing protocols are vulnerable to security attacks, as they are easily intercept able [21], this can severely deteriorate the performance and effective throughput of the network.

In this research, AODV routing protocol performance is studied in the presence of two severe security attacks (flooding attack [12] and black hole attack [14]). NS-3 [18] (Network Simulator 3) is used to simulate a MANET environment with wireless nodes running AODV protocol. Flooding and black hole attacks are simulated to show the effects of these attacks on the network in terms of packet drop ratio, transmission delays and routing overheads.

Then, we have implemented the widely used prevention schemes in order to improve the vulnerabilities observed in the existing protocol AODV. These prevention schemes used are FAP (Flooding Attack Prevention) and AMTT (Avoiding Mistaken Transmission Table) techniques. After that, these results are compared in order to analyze the improvements in network

performance. The proposed future work is to combine the existing protocols with some medium access schemes to improve the security vulnerability of MANET routing protocols.

The rest of the paper is divided into four sections. Section II will discuss the background of the AODV protocol, flooding and black hole attacks. Section III will explain the simulation scenarios and implementation discussion. Section IV will present the results and the discussion. Section V presents the conclusion and a brief about the future work.

2. Background And Previous Work

MANETs are typically infrastructure-less and autonomous networks [2] where a set of mobile nodes are connected by wireless adhoc links. The design of routing protocols for MANETs is complex because of several constraints. These routing protocol aim to provide paths that are not only optimum in terms of some standards (minimum distance, maximum bandwidth, and shortest delay) but also in satisfying some constraints, for example, the limited power of mobile nodes and the limited capacity of wireless links. The most widely used MANET routing protocols are AODV (Ad hoc On-Demand Distance Vector), OLSR (Optimized Link State Routing), and DSR (Dynamic Source Routing) [3]. The work in this paper only focuses to explore the security vulnerabilities related to AODV, such as the impact of flooding and black hole attacks.

2.1. AODV

AODV [4] is a reactive routing protocol because it can determine only on demand a route to the desired destination. The main features of AODV protocols are that it can recognize very quickly the link breakages and any changes in the network topology. AODV provides AODV [5] allows the nodes of MANETs to recognize very quickly the link breakages and also any changes in the network topology. It involves a wide range of operations, such as, route table management, path discovery, local connectivity management, and path maintenance [6]. The importance of this protocol is due to the presence of Route Discovery and Route Maintenance mechanisms [7]. Route Discovery depends on the RREQ (Route Request Message) and RREP (Route Reply Message). The route information of intermediate nodes is stored in the routing table entries. The route discovery mechanism is depicted in Figure 1, the sender initiates the route discovery by broadcasting the RREQ message. When the destination receives this RREQ, it will send a RREP message to the source of the RREQ. The TTEP message contains the complete route to the destination and next hop addresses are maintained to reach the destination. This mechanism prevents routing loops by using the sequence numbers in each routing table entry [8]. This can be helpful to determine whether the routing information in these tables is up-to-date. However, Route Maintenance depends on the RRER (Route Error) message and this can handle the dynamic network topology in MANETs. The RERR message, also maintain the routes by sending notification to the other nodes about a link failure [9]. AODV operation does need these types of messages to be disseminated [10]. Figure 1 shows example of an ad hoc network. This network has 14 active nodes, the source is node 1 and the destination is node 14. Node 1 will broadcast a RREQ message through the network until delivered to the destination. Complete description of the RREQ, RERR and RREP messages are given in [9], [10].

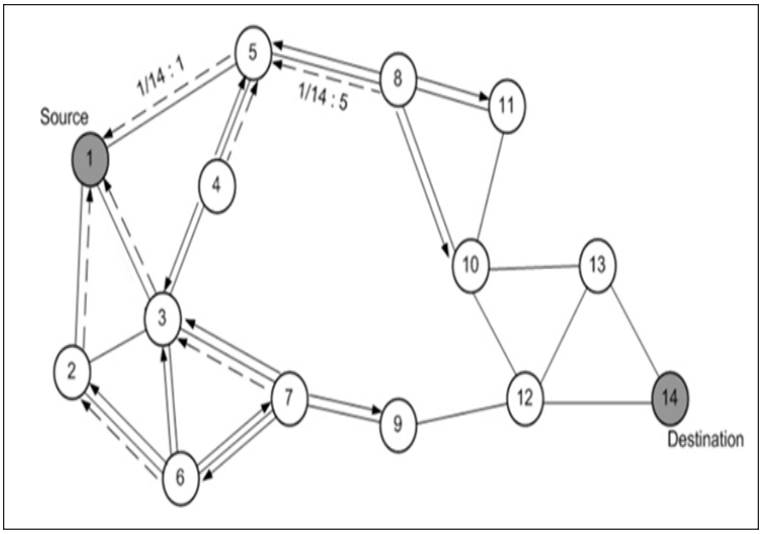

Figure 1. AODV Route Request (RREQ) mechabnism [9]

2.2 Security Threats

AODV has very limited capability to prevent against security threats. An attacker can exploit several vulnerabilities of AODV, such as absorbing routing packets, modifying and forwarding, false reply or sending false route request messages [11]. In this paper, we are limited to only two types of attack flooding and black hole attack. We will present a comparison on the impact of these attack on the AODV based MANETs.

2.2.1 Flooding

The goal of a flooding attack is to degrade the MANETs performance by flooding it with large amounts of traffic to disrupt the routing discovery or the maintenance phase within a MANET [12]. This attack is launched in AODV by sending multiple RREQs to non-existing destination nodes in a short time through RREQ flooding or routing table overflow as shown in Figure 2. This means that the malicious node represents false routes to all authentic nodes within this network.

The role of this malicious node is to prevent the creation of new actual ones; consequently, it causes routing table overflow by the authentic users. The avalanche of RREQs all over the network leads to the consumption of battery power and network bandwidth, causing DoS (Denial of Service) [13]. This can severely degrade the network throughput and performance.

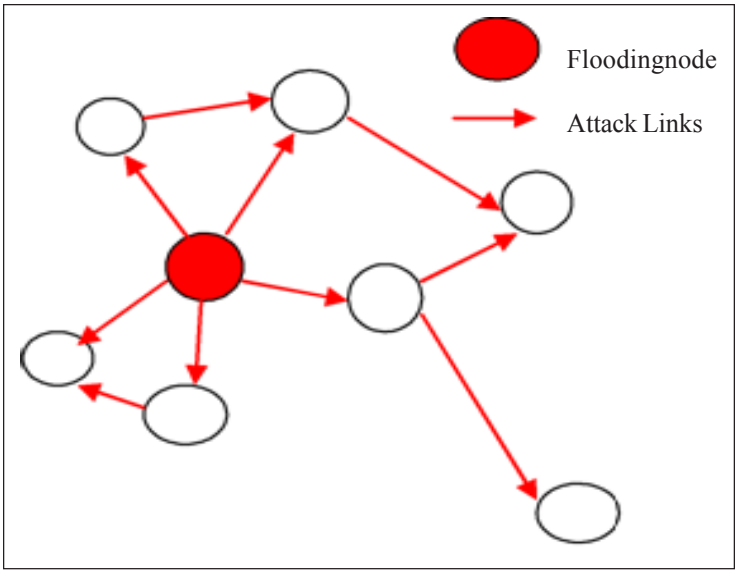

Figure 2. Flooding Attack Scenario

2.2.2 Black Hole Attack

The aim of a black hole attack is to spuriously reply to any RREQs without having an active route to the precise destination, and to drop all the received packets [14]. An attacker generates a Black hole attack and is able to modify the network topology by creating an auspicious "environment" for the attack. This is accomplished by forging RREQ messages [15] and advertising itself as having the shortest path for the packet to be delivered to the destination, in order to intercept the packets between two authentic nodes. Figure 3 how the black hole attack works. In the beginning, the originator node sends RREQs to the network to discover valid routes. A malicious node intercepts a RREQ, sent by the source node; this node then forwards it to the destination node and sends a RREP back to the source node to register itself as a legitimate route. After that, the source node transfers the data packets as an authentic user within the MANET. Then this malicious node intercepts the data flow by receiving the information but without forwarding it to the destination node. Obviously, the neighbor nodes are able to detect the sequence of the falsified RREQ or RREP messages sent by the malicious node, and then they put the malicious node in their blacklists by terminating the data flow over it [17]. It has been observed that by minimizing the exposure risk, the malicious node/s cannot intercept the data transfer between two related nodes, but still able to transmit the packet/s. Furthermore, the attacker can adequately amend some messages sent from particular nodes, though not from all.

2.2.3 Preventive Schemes

1) AMTT (Avoiding Message Transmissionables): AMTT is a technique was first proposed in [16]. Normally AODV uses FIFO rule to transmit route requests to neighbors. AMTT use the rule of priority instead of FIFO; the priority is inversely

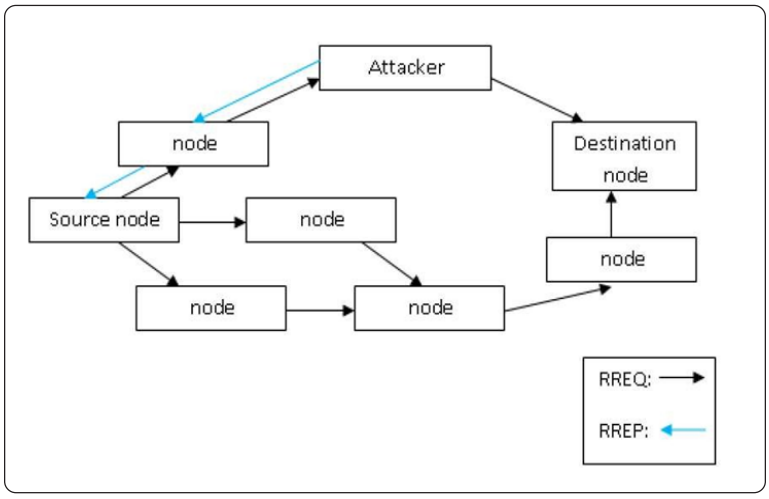

Figure 3. Black Hole Attack

proportional to the frequency of RREQ originated by a neighbor and compared to a threshold (Threshold is the number of RREQ allowed in a given time). If the frequency of the RREQ generated by a neighbor exceeds the threshold the neighbor is blocked for any more RREQ's, this was firstly proposed in 2006. In this scheme as mentioned in [16], "Legal nodes can distinguish illegal nodes and refuse to forward packages for them, so flooding attack can be defended".

2) FAP(Flooding attack Prevention): FAP is a technique that has been proposed firstly by [20]. This scheme has two methods to resist the flooding attack in Ad Hoc network. Firstly, to suppress the neighbors, this method is used to prevent RREQ flooding attack. Since the MANETs are multi-hop wireless networks, the node can send and receive packets from its neighbor nodes. If these neighbor nodes around the node refuse to receive its packets, this node cannot communicate with the others in MANET. By this way, the node has been isolated from the other nodes in the network, this is known as neighbor suppression and shown in Figure 5.

2.2.4 NS-3

In this research, the simulation tool used for analysis is NS-3.14. This simulator is highly preferred for academic networking research since it demonstrated the best overall performance [18].

3. Simulation and Scenarios

The experiments were setup to understand the severity of flooding and black hole attacks on MANET nodes running AODV protocol. The topology is explained in next section.

3.1 Topology

The simulation environment uses Wireless ad hoc network, which consist of 50 nodes. The nodes are users of Wi-Fi physical and MAC layer and the nodes move in a random walk based on the Gaussian Markov Mobility Model [19]. In this model, the velocity of the mobile node is assumed to be correlated over time and modeled as a Gauss-Markov stochastic process. The nodes are set to move with a mean velocity and direction based on a uniform distribution, this model best describes the real world MANETs.TCP is enabled at the wireless nodes to simulate the SYN Flooding attack. The wireless nodes use Wi-Fi physical and MAC layer, the Wi-Fi channel is modeled as a fading channel as implemented in NS-3 by Yans WifiPhy helper. At the Internet layer (IP), routing in conjunction with AODV for wireless routing is used. The ns-3 has derived AODV as a sub- class of the Ipv4Routing main class, hence AODV inherits all the functions which are part of the Ipv4 routing and plus the extra methods and functions which are specific to the AODV protocol.

3.2 Performance Parameters

We recorded three parameters to analyze the performance of AODV nodes under variable rate flooding and black hole attack.

1) **Average Time Delay:** The delay refers to the time it takes to transmit a packet from its source to its destination, and this time is

expressed in seconds. This value is attained by total transmission time divided by the number of packets received. This value is attained by using Delay Jitter Estimation class in NS-3. A time tag is attached to each packet transmitted and when it reaches the destination this information is subtracted from the simulator::Now function which keeps track of the current time.

2) **Routing Over Head:** This is calculated by Total no of routing bytes transferred over Total no of routing bytes +Total no of data bytes

Overhead = total routing bytes / (routing bytes + data bytes)

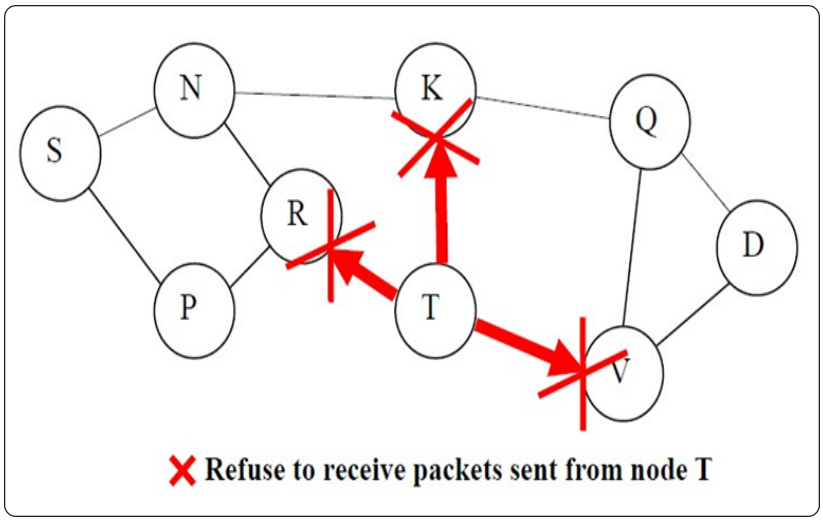

Figure 4. Neighbour Suppression

3) **Packet Drop Ratio:** This is the ratio of the total number of transmitted packets to the total number of received packets; this is expressed in terms of percentage so the resultant number is then multiplied by 100.

3.3 Node Types

For the flooding attack, we set up three different scenarios to see the effects of flooding based on node positioning, the type of flooding and valid data packets. Four different types of nodes were used in the simulation. Nodes can have three different roles in these simulation studies:

1) **Message Transmitting Node:** Wireless nodes sending UDP packets on a user defined port; the transmission is either a unicast message to a particular host or broadcasting to all the nodes on the network.

2) **Message Receiver Nodes:** These nodes were only listening and receiving the messages on a well-known port, i.e. 80.

3) **Flooding Nodes:** These are similar to the AODV wireless nodes with a difference that they flood UDP packets on MANET and the destination port is unknown. The flooding nodes were either transmitting to a particular node (unicast) or broadcasting to all the nodes.

4) **Black Hole Malicious Node:** This node will work as a black hole node, which consumes information and generates fake RREP messages.

3.4 Scenarios

The values chosen for these parameters in running the experiments are the inter-packet interval of flooding messages varied between 1.2 to 0.1 seconds. The reason behind this variance (from the biggest to the lowest number) is to observe the impact of flooding increase on the network performance (the results shown in Figure 7-15).

The three scenarios are as follows:

1) **Scenario 1:** All the valid data packets and the flooding packets were broadcasted on the network, this was used to analyze the effect of flooding on nodes which work as central or relay nodes.

2) **Scenario 2:** All the flooding packets were broadcasted but the valid data messages were unicast. This was used as a measure to find the effect of the flooding on the one to one communication between nodes.

3) **Scenario 3:** The third scenario was setup with both the flooding node and the data transmission nodes sending the messages to a similar node. This was done to analyze the impact of flooding on the processing times of a receiver node which is receiving valid as well as malicious messages.

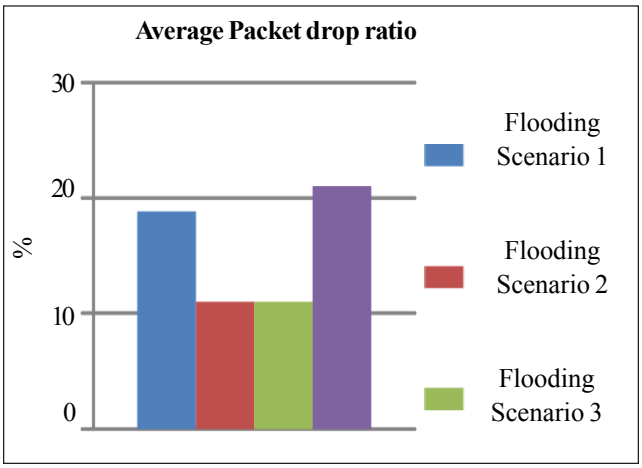

Figure 5. Comparison of Packet drop ratio

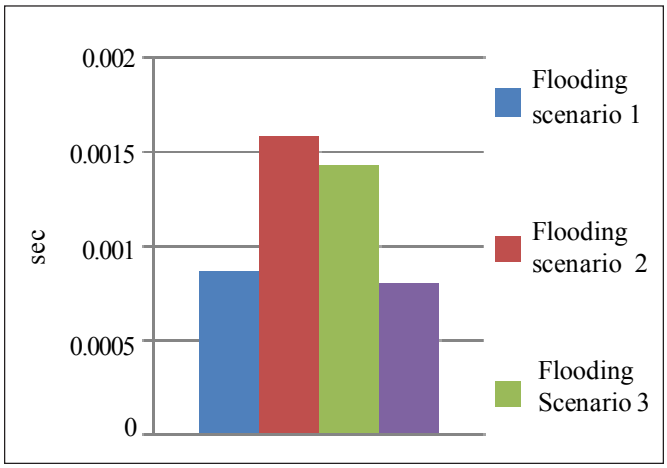

Figure 6. Comparison of Packet delay

4) **Malicious Node Scenario:** To analyze the behavior of a black hole attack. Malicious nodes are placed in vicinty of different participating nodes. In the black hole attack valid routing packets are dropped and malicious routing packets are generated hence the position of the node in the network is very important. This is why we chose differently located nodes with various mobility directions and analyzed the impact on the network performance.

Scenarios	Average Packet Delay(sec)	Average Drop Ratio(%)	Routing Overhead (%)
FloodSc1	0.0009	18	55
FloodSc2	0.0016	11	69
FloodSc3	0.0014	11	69
Black hole	0.0008	21	49

Table 1. Statistics for security attacks

4. Results

We compare three different set of experiments. Initially the packet drop ratio, average time delay and routing overhead was measured without any attacks for reference. The second set of experiments were conducted with the three different flooding and a black hole attack scenario. The last sets of experiments were with similar attack scenarios but using either FAP or AMTT protection. Figure 5-6 and Table 1 depicts the results in case of all three flooding and a black hole attack. All these change in averages of packet drop, time delay and routing overhead is compared to normal network operation. The results clearly indicate worsening of network performance in attack scenarios. The results for the flooding attacks show a higher average packet delayand routing overhead as compared to black hole attack. The packet drop ratio for flooding scenario 1 and black hole attack is worse than the other flooding scenarios. Figure 7-15 and Table 2 (prevention stats) shows the statistics for the no attack scenario, all the three different flooding scenarios, and with AMTT and FAP prevention implemented separately. AMTT increases the network throughput, compared with FAP, i.e. low packet drop ratio. However, AMTT has a higher routing overhead and

prevention schemes have their pros and cons and the choice of each depends on the application scenario/s. In addition, we observed that flooding attack severely depreciates the network performance by dropping valid data packets ranging from 4% to 70% as proportional to the frequency of flooding packets.

Scenarios	Average Packet Delay(sec)		Average Drop Ratio(%)		Routing Overhead (%)	
	FAP	AMTT	FAP	AMTT	FAP	AMT T
FloodSc1	0.0009	0.001	11.6	10.4	49.9	51.3
FloodSc2	0.0013	0.0015	8.88	7.48	68.2	71.8
FloodSc3	0.0013	0.0012	8.27	7.17	67.5	67.9

Table 2. Statistic with prevention scheme

5. Conclusion

This work deals with monitoring the AODV protocol performance for use in MANETs. We showed different scenarios of flooding attack and black hole attack on a MANET with 10 nodes, which are connected on wireless network with random walk.

The network performance was evaluated based on packet drop ratio, average packet delay and routing overhead with implementation of no attack and attack scenarios in ns-3. We chose three different flooding attacks with broadcast and unicast packets. The flooding attack severely deteriorates the network performance, packet drop ratio of between 70 to 100% in the unicast scenario. The black hole in comparison had a lower packet drop ratio. Also, average packet delay and routing overhead increased with flooding attack and had a severe effect on the network performance. This work looks into different prevention schemes, which can be effective for countering flooding attacks.

We then choose two existing techniques, FAP and AMTT. The results from the FAP showed up to 30 to 35% improvement in packet drop ratio. The average packet delay in some scenarios increases with FAP prevention because of the extra processing time to segregate flooding packets from valid data packets. The routing overhead improves with FAP prevention because the scheme identifies the route from the flooding nodes as malicious and the routing packets, then at the neighboring nodes, are dropped. Similarly, with AMTT, the packet drop ratio has shown some improvement in comparison with FAP; an average decrease of 6 to 10% in the packet drop ratio is observed; however, this comes with a penalty. The timing delays increased to a level of 0.5 to 0.7 ms; also the complexity and the memory usage is quite high. On the other hand, the routing overhead is minimal, when compared to FAP. This is because a similar amount of routing updates and error messages are required as in FAP, but without any overheads.

References

[1] Perkins, C., Elizabeth, B. R., Das, S. (2003). Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, July.

[2] Chlamtac, I., Conti, M., Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges, *Ad Hoc Networks*, 1 (1) 13–64,

[3] Zhang, Z., Zhou, H. (2009). Empirical examination of Mobile Ad Hoc Routing Protocols on wireless sensor networks, *International Journal of Computer Networks*., 1 (1) 75–87.,

[4] Holter, K. (2005). Comparing AODV, OLSR, (2005). folk. uio. no/kenneho/studies/essay/essay. html, no. April, 1–19.

[5] Perkins, C., Royer, E. (1999). Ad-hoc on-demand distance vector routing, WMCSA'99. Second IEEE Workshop on.

[6] Gerasimov, I., Simon, R. (2002). Communication Support for Tightly- coupled Distributed Mobile Applications, International *Journal of Simulation*, 23–39.

[7] Zahary, A., Ayesh, A. (2008). On-demand multiple route maintenance in AODV extensions (ORMAD), 2008 International Conference on *Computer Engineering & Systems*, 225–230, November.

[8] Marina, M. K., Das, S. R. (2006). Ad hoc on-demand multipath distance vector routing, Wireless Communications and Mobile Computing, 6 (7) 969–988, November.

[9] Solheid, A. (2005). AODV enhanced by Smart Antennas, fundp.ac.be.

[10] Perkins, C. Ad hoc On-Demand Distance Vector (AODV) Routing. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt.

[11] Ning, P., Sun, K. (2005). How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols, *Ad Hoc Networks*, 3 (6) 795-819.

[12] Yu, J., Lee, H. (2008). Traffic flooding attack detection with SNMP MIB using SVM, *Computer Communications* 31. 17, 4212-4219.

[13] Ngadi, M., Khokhar, R., Mandala, (2008). A review current routing attacks in mobile ad-h oc networks, International *Journal of Computer Science and Security*, 2, p. 18–29.

[14] Goyal, P., Parmar, V., Rishi, R. (2011). MANET: Vulnerabilities, Challenges, Attacks, Application, *International Journal of Computational and Management*, 11, January, 32–37.

[15] Esmaili, H., Shoja, M. (2011). Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator. arXiv preprint arXiv:1104.4544.

[16] Li, S., Liu, Q., Chen, H., Tan, M. (2006). A New Method to Resist Flooding Attacks in Ad Hoc Networks, 2006 International Conference on Wireless Communications, *Networking and Mobile Computing*, 1–4, September.

[17] Ullah, I., Rehman, S. (2010). Analysis of Black Hole attack on MANETs Using different MANET routing protocols, A Mater Thesis, *Electrical Engineering*, thesis no MEE, 10, 62.

[18] Weingartner, E., Vom, L., Wehrle, K. (2009). A performance comparison of recent network simulators, *In*: Communications, ICC'09. *IEEE International Conference on* (1-5).

[19] Henderson. M. (2008). Network simulations with the ns-3 simulator, SIGCOMM demonstration.

[20] Ping, Yi., et al. (2005). Resisting flooding attacks in ad hoc networks. Information Technology: Coding and Computing, ITCC 2005. International Conference on. 2. IEEE.

[21] Priaynka, G., et. al. A literature review of security attack in mobile ad- hoc networks, *International Journal of Computer Applications*. 9, 11-15.

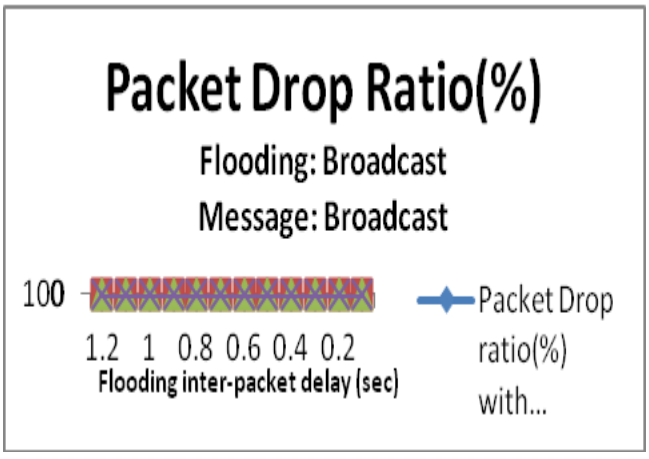

Figure7. Packet Drop Ratio for Scenario 1

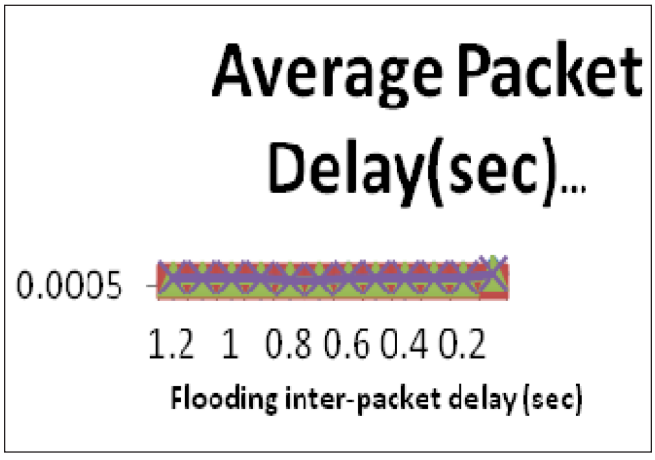

Figure 8. Packet Delayfor Scenario 1

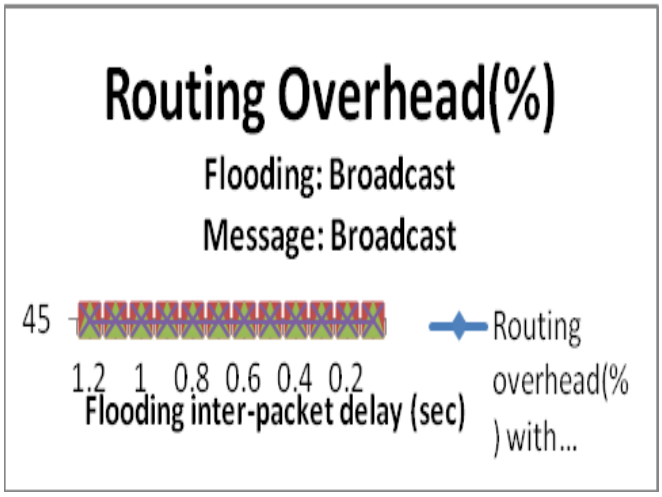

Figure 9. Routing Overhead for Scenario 1

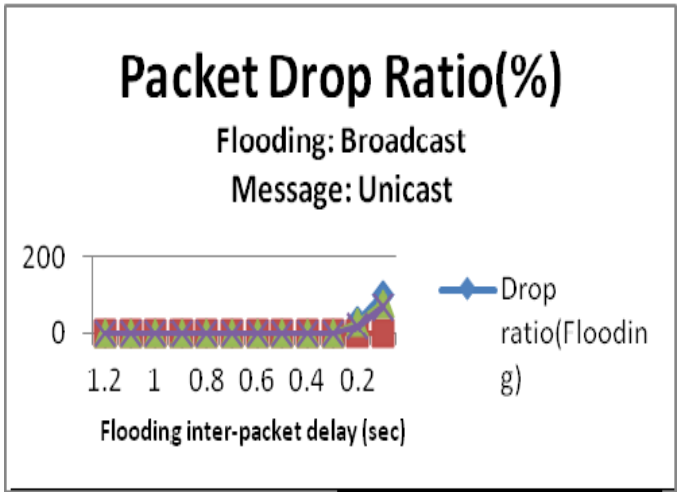

Figure 10. Packet Drop Ratio for Scenario 2

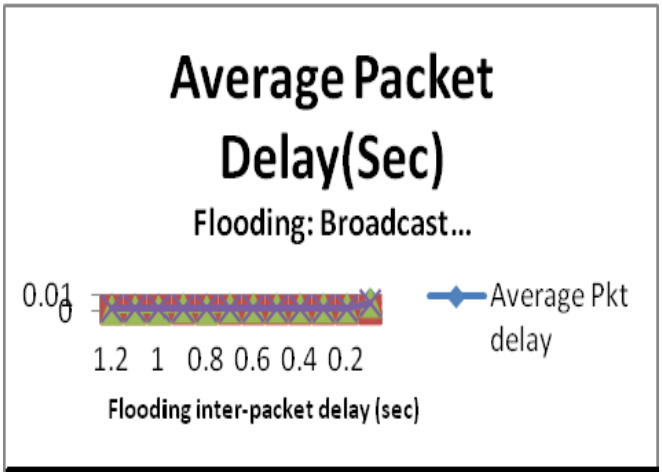

Figure11. Packet Delay for Scenario 2

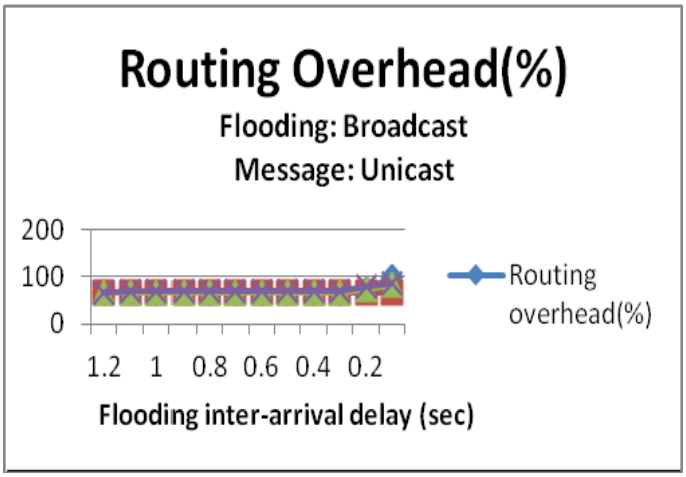

Figure 12. Routing Overhead for Scenario 2

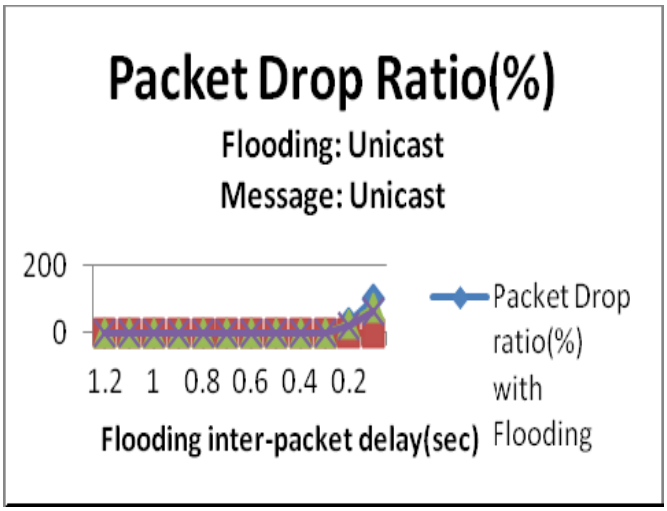

Figure13. Packet Drop Ratio for Scenario 3

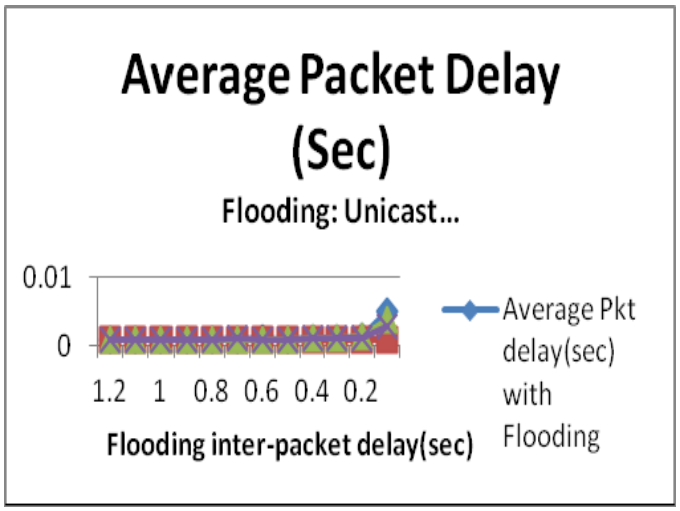

Figure14. Packet Delay for Scenario 3

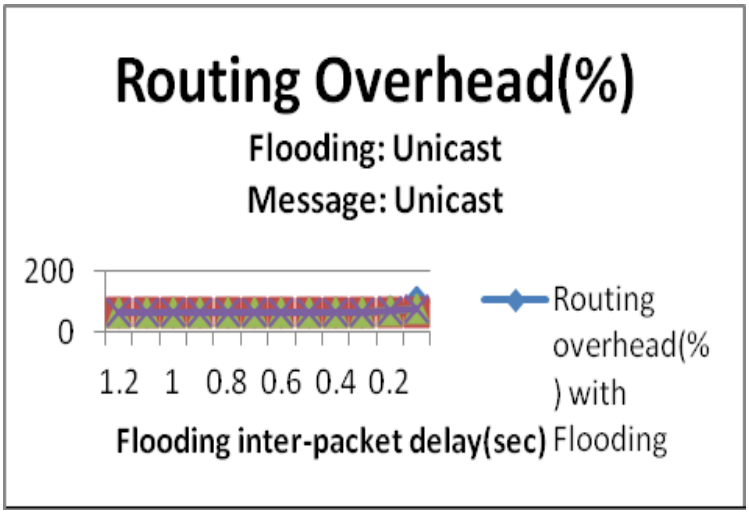

Figure 15. Routing Overhead for Scenario 3