ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/291321526

Performance and Security Analysis for Proactive and Reactive Protocols in Mobile Ad-hoc Network

Conference Paper · September 2014

CITATIONS
0

READS
72

4 authors:

Malek Najib Omar
3 PUBLICATIONS **8** CITATIONS
SEE PROFILE

Ibrahim Thorig
Maldives National University
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Mazleena Salleh
Universiti Teknologi Malaysia
113 PUBLICATIONS **1,037** CITATIONS
SEE PROFILE

Mohammad Abdur Razzaque
Teesside University
70 PUBLICATIONS **1,690** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Lightweight Cryptography for device level security in IoT devices View project

yousra abdul alsahib s.aldeen View project

All content following this page was uploaded by Malek Najib Omar on 20 January 2016.

The user has requested enhancement of the downloaded file.

IRICT 2014
1st International Conference of Recent Trends in Information and Communication Technologies

Performance and Security Analysis for Proactive and Reactive Protocols in Mobile Ad-hoc Network

Malek Najib Omar *, Ibrahim Thorig, Mazleena Salleh,

Mohammad Abdur Razzaque

Faculty of Computing, University Technology Malaysia, Malaysia

Abstract

This paper discussed about two proactive protocols which are DSDV and OLSR as well as two reactive protocols which are AODV and DSR. In addition, security analyses have been conducted and it covered the possible attacks that can be implemented against Mobile Ad-hoc Network (MANET). Furthermore, analysis and the comparison studies of the routing protocols in MANET that is conducted by simulation are discussed. The metrics have been used to compare these routing protocols are throughput, end to end delay, packet delivery ratio fraction verses the number of nodes in AODV and DSR. A black hole security attack was simulated and analyzed for DSDV, AODV and DSR. This study also investigated the impact of the increased in number of nodes used in the simulation to have more accurate results for the analysis.

Keywords. MANET; Proactive; Reactive; Hybrid; Attacks; Black hole attack.

1. Introduction

There are mainly three types of ad hoc routing protocols in a mobile network which are table-driven, on demand-driven and hybrid routing protocols. Such protocols are designed to solve typical limitations of networks such as high power consumption, low bandwidth and high error rates. Figure1 below illustrates the categorization of ad-hoc routing protocol.

*Corresponding author: malek2omar@hotmail.com

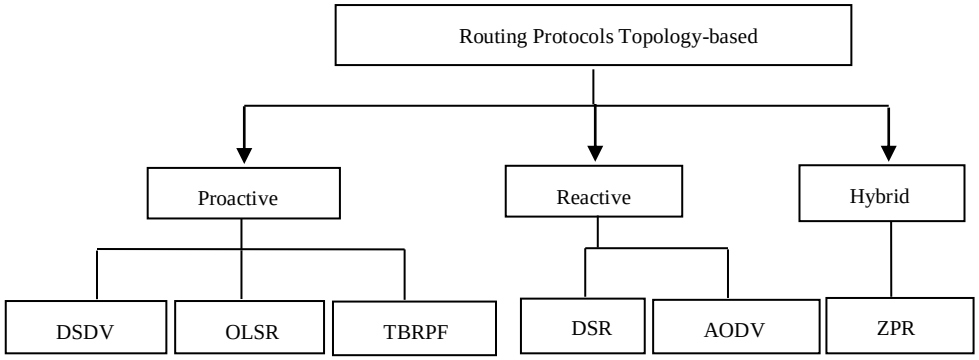

Fig.1. Categorization of ad-hoc routing protocol

These three routing types are topology based and elaborated as the following:

1. Table-Driven Routing Protocols – Proactive

Table-driven routing protocols are proactive routing protocols. Nodes in the networks are updated by consistently forwarding routing information one node to another. Therefore, it requires large routing tables. Destination-Sequenced Distance Vector (DSDV) is one type of table-driven routing protocols.

2. On Demand-Driven Routing Protocols - Reactive

A different approach from table-driven routing protocols is on demand-driven routing protocol. It is also called reactive routing protocol. The routing process only focuses on routes from source to destination. The protocol will start to discover the route within the network if the source nodes require a route to destination. Therefore, it requires small or no routing tables. Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are examples of on demand-driven routing protocols.

3. Hybrid Routing Protocols

Hybrid routing protocols are the combination between table-driven and on demand-driven routing protocols. Hybrid routing protocols was used for several purposes. One of them is to combine the advantages between the proactive and reactive routing protocols. Zone Routing Protocol (ZRP) is a typical hybrid routing protocols.

Dynamic Source Routing (DSR) was proposed by Broch, Johnson and Maltz for Mobile Ad-Hoc Network (MANET). Full source-route is aggregated in Route Request and sent back in Route Reply. The protocol requires each data packet to carry the full address for all nodes along the path. If the route to another node is unknown, it will initiate a route discovery process by sending many requests of route request (RREQ) packets. Each node receives the RREQ packets will reply to the RREQ message by sending the route reply (RREP) packet. However, the route to the destination node can be taken from its cache if the target node is already known. The RREQ packet will establish traverse path from destination to the source node. The RREP packet will use the path to reach the source node. The route error (RERR) is used to inform about any broken link within the network. This route information will be discarded from the cache. DSR routing protocols have several advantages against other protocols. It can store multiple routes in the route cache that eliminate a route discovery process. Route discovery is not needed if the source node found a valid route in its route cache. The protocol will be very effective in a network with low mobility since it will keeps route information for long period.

Ad hoc On Demand Distance Vector (AODV) routing protocol is similar to DSR. It implements route discovery procedure to communicate with unknown nodes. The protocol is implemented based on DSR algorithm. There are two major differences that can be used to differentiate between DSR and AODV. Firstly, full routing information is carried out by the packet in DSR; whereas in AODV, it only carries the destination address. Secondly, the route replies (RREP) in DSR will carry the address of every node along the path, whereas the route replies (RREP) in AODV carry the destination IP address and the sequence number only.

The route discovery of AODV protocol is performed as bellow:

1. Source node broadcasts RouteRequest packet.

2. Each intermediate node gets a RouteRequest will do the following steps:

    - Establish a reverse link to the source node.
    - If request received before → discard.
    - If route to destination is available and up-to-date → return RouteReply using the reverse link.
    - Otherwise → rebroadcast the RouteRequest.

3. Destination node responds with RouteReply using the reverse link.

Destination-Sequenced Distance Vector (DSDV) is a driven-table proactive routing protocol which is using the Bellman-Ford algorithm to calculate paths [1]. The cost metric in DSDV is hop count, which is the number of hops that the packet will use to reach its destination. DSDV keeps the routing table for all the nods of the network. Moreover, DSDV uses periodic and triggers updates to maintain the routing table corrected and efficient in the networks. Due to this updates, routing loops can be occurred in the network. However, the nodes that use DSDV will be triggered with a sequence number to eliminate the routing loops in the network. When a periodic update occurs, the nodes will increase the sequence number by 2 and add the updates information to the routing message. Moreover, when the node desires to send an update for an expired route, the node will increase the sequence number by 1. In this case the nodes which receive this update will eliminate the expired route from the routing table. In DSDV, the nodes cannot change the sequence number from other nodes.

Optimized Link State Routing (OLSR) [2] is a proactive protocol. It means, the path from the source to the destination is discovered and saved before sending the packets. In OLSR, the link state information is discovered by propagating HELLO messages and topology control TC. When the node receives this information, it will process to calculate the next hop for all the nodes in the networks. HELLO messages are able to discover two-hop neighbor information and select a set of multipoint relays (MPRs). Furthermore, transmitting the messages and constructing link state are the responsibilities of MPRs. OLSR makes sure that all the nodes are updated with the link state by flooding the topology data frequently through the network.

2. Related Work

Pradish Dadhania *et. al.*, [3] evaluated the performance of AODV and DSR routing protocol under black hole attack. The author of the paper used NS2 to simulate the mobile network environment. The node starts at a random position, waits for the pause time, and then moves to another random position. The size of the packet is 512 bytes and a transmission rate is 4 packets. The simulation setup consists of such nodes without attack and nodes with the attack. Three parameters have been chosen in this simulation which consists of throughput, end to end delay and packet delivery ratio. The performance of AODV and DSR are affected very badly during the black hole attacks.

D. Deepthi Veronica *et. al*., [4] evaluated various MANET routing protocols such as AODV and DSR. Three network parameters have been chosen in the simulation consists of packet delivery fraction, throughput and end to end delay. As usual, NS2 has been used to simulate and evaluate the performance of AODV and DSR. Two experiment scenarios have been setup in the paper with different specific values. The number of nodes in first scenario was 9, whereas the number of nodes in second scenario was 16. The graph or results are varying between AODV and DSR.

Sahil Gupta *et. al*., [5] examined the performance of popular reactive protocols. AODV and DSR were respectively tested based on variation of node density and mobility. Throughput and average end to end delay were the parameters used to determine the performance of the AODV and DSR based on the increasing node density. The experiment conducts two types of scenarios consist of varied nodes density and pause time. Higher node in AODV showed an extreme degradation performance of the routing protocols itself.

Rachit Jain *et. al*., [6] analyze the behavior of several routing protocols like AODV and DSR with path loss propagation models. Popular performance metric such as throughput, average end to end delay, average jitter and packet delivery fraction have been chosen in the simulation experiments. The main contribution of the project is to choose the correct protocol for any active operating environment.

Nisarg Gandhewar and Rahila Patel [7] evaluated the performance of AODV by simulating the routing protocol in NS2. Different metrics were chosen in the simulation experiments consists of average end to end delay, packet delivery ratio and packet loss. The numbers of nodes were varied in each parameter. The performance of AODV protocol was extremely degraded when the numbers of nodes are increased.

S. Mohapatra *et. al*., [8] conducted a simulation experiment to evaluate the performance of AODV, DSR, OLSR and DSDV protocols using NS2 simulator. The parameters were chosen in the simulation consists of delay, throughput, control overhead and packet delivery ratio. These parameters were tested with different number of nodes, different speed (pause time) of nodes and different size of network. The authors run 10 random simulations to produce 10 random scenario patterns. The results of the scenario pattern generate 10 outputs.

Umadevi Chezhian and Raja Adeel Ahmad [9] analyzed two types of parameters which are average delay and throughput to evaluate the performance of Ad Hoc Network Protocols such as AODV, DSR, TORA and DSDV. The researchers used different network size, pause times and mobility velocity. The result of each routing protocol are varied between each other due to the changes of the network size and pause time.

Many other researchers have simulated related MANET proactive protocols for DSDV and OLSR such as performance evaluation for DSDV and OLSR. The researchers considered the throughput, end to end delay (E2ED) and normalized routing load (NRL) [10]. Some researchers evaluated and compared the Packet Delivery Ratio (PDR), Normalized Routing Overhead (NRO) and average E2ED for DSDV and OLSR [11].

Other researchers conducted performance comparison of the throughput, packet drops and the TCP variants over DSDV and OLSR [12]. Others present the path loss model and comparison for DSDV and OLSR above 802.11 and 802.11p [13].

Another related works were simulated a novel attack on DSDV routing [14]. Also some other researchers simulated the performance and evaluated DSDV on TCP and UDP environments. These researchers examined the throughput of the received packets, throughput of the dropped packets, E2ED, packet delivery fraction and routing load [15].

Besides, simulated and compared DSDV, AODV and DSR in 802.11 MAC for grid topology in MANET with consideration for the metrics of E2ED Vs. no. of nodes, received packets Vs. no. of nodes, packet delivery ratio Vs. no. of nodes and total dropped packets Vs. no. of nodes [16]. Furthermore, some researchers simulated and compared AODV, DSDV and DSR with the some metrics such as Average energy consumption, normalized routing load and average of throughput [17].

3. Routing Attacks Analysis

This section discusses the attacks against MANET routing protocols in general. Moreover, it elaborates the attacks that could be used against DSR, AODV, DSDV, and OLSR as well.

3.1 Flooding Attack

In this attack, the attacker aims to reduce the networks performance by exhausting their resources [18]. The attacker tries to increase the bandwidth in the network, consumes the nodes resources such as a battery power and processing more operations. This attack will reduce the network performance. For instance, a malicious code in AODV protocol is able to send a huge numbers of RREQs to a fake destination or to a node which is not existed in the network. Therefore, a flood of RREQs is sent to all the nodes in the network which consumes the battery power of the nodes and the bandwidth of the network as well. Consequently, this flood attack can lead to denial of a service.

3.2 Replay Attack

MANET does not have fixed infrastructure, also the mobility of MANET nodes is one major characteristic in the network. Therefore, one of the nodes may not be existed anymore in the network or out of range. Moreover, a node A records node's B valid control messages to resend it later while node B is already out of range. Therefore, other nodes in the network would update their routing table with stale and expired routing information [19]. In addition, Replay Attack may be used to impersonate a specific node which no longer exists in the network of MANET.

3.3 Wormhole Attack

A wormhole attack is sophisticated attack in MANET. A wormhole attack can be implemented using private high speed network. Two attackers are working together to record packets at one location, and then they forward those packets at different locations [20]. Wormhole attack will make other nodes record incorrect routing information in their routing tables. It is really serious matter that wormhole attack can be implemented against all the communications that provide confidentiality and authenticity.

3.4 Black hole Attack

In the black hole attack, the attacker tries to gain all the packets from the source [21][22]. The attacker will use a malicious node to gain all the packets from the source by suggesting a fake route through itself. The malicious node will suggest better route than other nodes to convince the source node that its route is the best. Therefore, the source node will choose the malicious node as the best way to the destination. So, the attacker will receive all the packets that come from the source node. Moreover, the attacker will be able to drop the entire received packets. For instance, in AODV, the malicious node will response for RREQ from the source and

it will reply with the best RREP to the source. Therefore, the source will believe that the malicious node is the best hop count to reach to the destination.

3.5 Gray hole Attack

The gray hole attack has the same implementation steps of the black hole attack. Therefore, the attacker will use a malicious code with showing the best path to have all the traffics. However, the difference between the black hole and the gray hole is that the black hole attack will discard or misuse all the received packets while the gray hole attack will forward the received packets to the destination [22].

3.6 Link Spoofing Attack

In this attack, the attacker uses a malicious node to cheat the target node with a fake or non-existed link. So, the target node will choose the malicious node to send the data to the destination [23]. For example, in OLSR, the malicious node will show the best link state to the destination, so that the target node will believe that the malicious node is the best way to the destination. Therefore, the malicious node will be the target node MPR. The MPR malicious node will receive all the packets from the target node. Therefore, it will be able to modify the received packets or discard all of them.

3.7 Link Withholding Attack

In link withholding attack, a malicious ignores the requirement to advertise a link state to one or more nodes in the network. This attack will lead to link lose and communication lost to the targeted node. Link withholding attack will make the other nodes in the network unable to see the targeted node in the advertisement of the malicious node. This attack is considered as serious matter in link states protocols.

3.8 Collusion Attack

In this attack, two or more attackers work in collusion with each other to disrupt the routing process. The attackers aim to modify or drop the received packets from the targeted node. Collusion attack is difficult to be detected by using some conventional techniques such as *pathrater* and *watchdog* [23]. For example, a targeted node sends the packets to X malicious node. X malicious node is forwarding the received packets to Y malicious node as usual to avoid any detection from the targeted node. Therefore, malicious node Y will be able to modify or drop the received packets.

3.9 Selfish Behavior

MANET nodes are suffering from selfish behavior. The selfish behavior of MANET nodes prevents them from forwarding the received packets to the other nodes in the network. The reason of this behavior is the nodes are trying to preserve their resources from being exhausted [24]. For instance, node A participates in all the operations in the network. However, node A will not forward the received packets for some reasons such as consuming its battery life.

3.10 Broken Link Fraud Attack

Broken link fraud attack is aimed to prevent a route to one of the legitimated nodes in the network by advertising a broken link fraud [25]. For example, in DSDV, one of the nodes misbehaves and advertises that one node is not reachable. The misbehaved node or the malicious node assigns the hop count as infinity in its routing table. Then the malicious node advertises this broken link fraud to all the other nodes. Therefore, the other nodes update their routing table according to the malicious code false information. In this case, the targeted node will be assigned as infinity in the other nodes routing table. Therefore, all the nodes in the network will consider the targeted node as non reachable node. So, the targeted node will not be used anymore for forwarding any information.

4. Methods

The following performance metrics have been used in the simulation and the analysis as well:

4.1 End-to-End Delay

Delay occurs in specific pair communicating of nodes and it is also caused by the data-rate of the link. The delay of packet transmission can be explained as the time taken for a bit of data to travel from one node to another node. All the bits take a time to travel across the network from one node to other nodes. End to end delay consists of Processing delay, Queuing delay, Transmission delay and Propagation delay. Such delays have different implementation methods in packet switching.

4.2 Throughput

Throughput can be defined as the amount of data transferred from one place to another in a specified amount of time. The data transfer rates for disk drives and networks are measured in terms of throughput and it delivers over physical link. Throughputs can be measured in Kbps, Mbps and Gbps. Maximum throughput of a device or network maybe significantly higher than the actual throughput achieved in everyday use. Several factors, such as Internet connection speed and network traffic may limit the data transfer.

4.3 Packet Delivery Fraction

The ratio of the data packets delivered to the destinations. The delivered data packets are generated by the CBR sources. Packets delivered and packets lost are taking into consideration as well.

4.4 Black hole Attack

It has been discussed in Section 3.

4.5 Normalized Routing Load (NRL)

Normalized routing load is the ratio between the numbers of routing packet which is sent over the network to the number of data packets received to the destination node [26].

5. Results and Discussion

5.1 Simulation Environment 1

The simulation and experiment were carried out in Ubuntu 12.04 with network-simulator-2 (version 2.35). For the topology generation NSG 2.1 script generator was used. And to generate information from data, awk scripting was used.

Traffic Model: Source and destination pairs were spread randomly and Continuous bit rate (CBR) traffic source used for the simulation.

Mobility Model: Node mobility was defined using random waypoint. Therefore, nodes freely move around the environment.

The experiment was carried out under following scenario:

Table 1. Scenario 1

Parameter	***Value (s)***
Network Type	Mobile
Connection pattern	Random
Number of nodes	50, 100, 150, 200
Simulation time	10s
Environment size	800 x 800
Connection pattern	Constant Bit Rate (CBR) / TCP
Packet size	512
Queue length	50
Protocols	AODV, DSR

Graphs of Figure 2 show the performance of AODV and DSR based on the simulation scenario. It shows that the average throughput of DSR is better than AODV when the number of nodes is increased. That means the amount of packets transferred per *ms* in DSR which is higher than AODV. Figure 3 shows that the amount of packets from source to destinations in DSR is higher than AODV as well as the consideration to the lost packets.

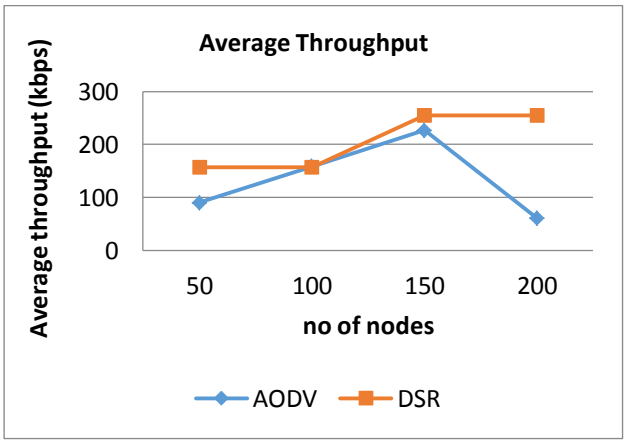

Fig. 2. Average of Throughput

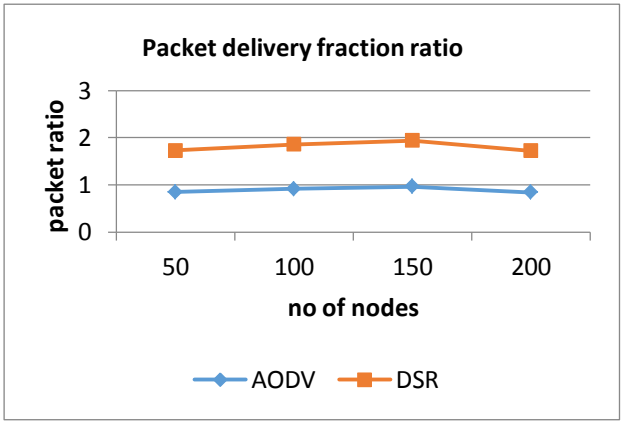

Fig. 3. Average of Packet delivery fraction ratio

In Figure 4, the time that DSR takes to deliver the data is higher than AODV; which means AODV has a lower ratio of delay. This makes AODV faster than DSR in delivering the packets.

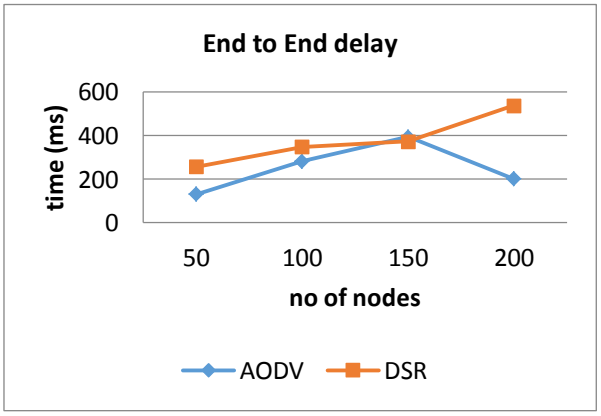

Fig. 4. Average of End to End Delay

5.2 Simulation Environment 2

Black hole attack was simulated to evaluate the performance of AODV, DSR and DSDV under an attack situation. Following parameters were used to simulate the black hole attack.

Table 2. Scenario 2

Parameter	***Value (s)***
Network Type	Mobile
Connection pattern	Random
Number of nodes	20, 50, 90, 150
Simulation time	450s
Environment size	700 x 700
Connection pattern	Constant Bit Rate (CBR) / UDP
Packet size	150
Queue length	50
Protocols	AODV, DSR, DSDV

In Figure 5, AODV, DSR and DSDV protocols were under the black hole attack. From the results, DSDV and AODV have almost similar values for the throughput. Moreover, both of DSDV and AODV have a smaller ratio of throughput for the delivered packets comparing to DSR. That means that DSR has more resistance for black hole attack. Figure 6 shows the normalized routing load for DSR is higher compared to DSDV and AODV. Moreover, DSDV and AODV have the same normalized routing load when they are under black hole attack. That means AODV and DSDV have more efficient route than DSR. Figure 7 show that DSDV and AODV have higher packet delivery fraction than DSR. DSDV and AODV have almost the same value which means both of them are better than DSR.

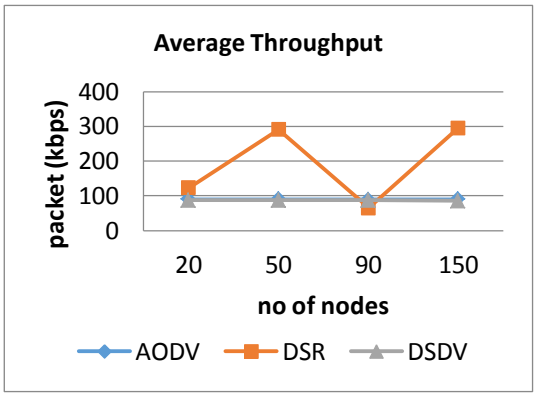

Fig. 5. Average of Throughput under Black hole attack

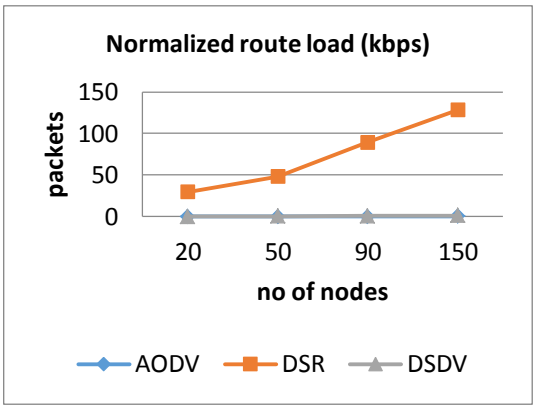

Fig. 6. Average of Normalization under the Black hole attack

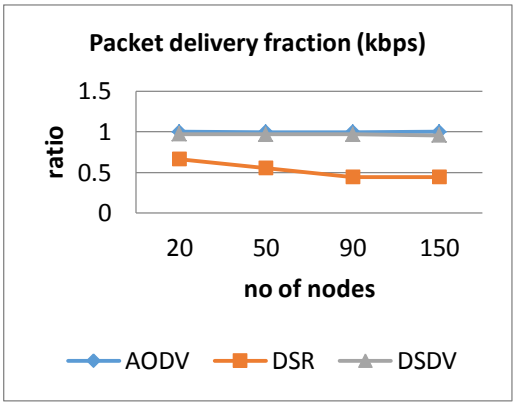

Fig. 7. Average of Packet delivery under the Black hole attack

6. Conclusion

In conclusion, this paper discussed the security attacks that MANET faces in the real world. Moreover, a performance analyses for DSR and AODV based on throughput vs. the number of nodes, the end to end delay vs. the number of nodes and packet delivery ratio fraction vs. the number of nodes. Moreover, in this paper, results through simulation of the black hole attack were generated and compared for DSDV, AODV and DSR. This research is more accurate than previous researches, because it increased the number of nodes used in the simulation compared to previous researches. In the near future, further simulations and solution will be introduced to continue the testing of the other security attacks for proactive and reactive protocols.

References

1. Perkins, C. E., & Bhagwat, P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM Computer Communication Review* Vol. 24, No. 4, pp. 234-244, October 1994.
2. Clausen, T., Jacquet, P., Adjih, C., Laouiti, A., Minet, P., Muhlethaler, P., & Viennot, L. Optimized link state routing protocol (OLSR), 2003.
3. Dadhania, P., & Patel, S., Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks. Performance Evaluation, 3(1), 1487-1491, 2013.

4. Deepthi Veronica, D., & Jagannadha Rao, D., Performance Analysis of AODV and DSR in MANETS Using NS2 Simulation. Performance Analysis, 1(4), 2320-9801, 2013.
5. Gupta, S., Arora, S., & Banga, G. Simulation Based Performance Comparison of AODV and DSR Routing Protocols in MANETS. International Journal of Applied Engineering Research, 7(11), 2012.
6. Jain, R., & Shrivastava, L., Study and Performance Comparison of AODV & DSR on the basis of Path Loss Propagation Models. International Journal of Advanced Science and Technology, 32, 2011.
7. Nisarg Gandhewar, & Rahila, P., Performance Evaluation of AODV protocol in MANET using NS2 Simulator. International Journal of Computer Applications, 2011.
8. Mohapatra, S., & Kanungo, P., Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator. International Conference on Communication Technology and System Design, 2011.
9. Umadevi Chezhian, Dr., & Raja Adeel, A., Average Delay and Throughput Analysis on Ad Hoc Network Protocols. 3(2), 2277 128X, 2013.
10. Wasiq, S., Arshad, W., Javaid, N., & Bibi, A., Performance evaluation of DSDV, OLSR and DYMO using 802.11 and 802. lip MAC-protocols. In *Multitopic Conference (INMIC), 2011 IEEE 14th International* (pp. 357-361), 2011.
11. Kumar, S., Javaid, N., Yousuf, Z., Kumar, H., Khan, Z. A., & Bibi, A., DSDV, DYMO, OLSR: Link Duration and Path Stability. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* (pp. 1862-1866), 2012.
12. Morshed, M., Rahman, M. U., Rahman, M., & Islam, M., Performance comparison of TCP variants over AODV, DSDV, DSR, OLSR in NS-2. In *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on* (pp. 1069-1074), 2012.
13. Mohammad, S. N., Wasiq, S., Arshad, W., Javaid, N., Khattak, S., & Ashraf, M. J. (2013, October). Modeling Probability of Path Loss for DSDV, OLSR and DYMO above 802.11 and 802.11 p. In *Broadband and Wireless Computing, Communication and Applications (BWCCA), Eighth International Conference on* (pp. 534-538), 2013.
14. Kaur, R., Gaur, M. S., & Laxmi, V., A novel attack model simulation in DSDV routing. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on* (pp. 1-5), 2011.
15. Vijaya, I., & Rath, A. K., Simulation and performance evaluation of AODV, DSDV and DSR in TCP and UDP environment. In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on* (Vol. 6, pp. 42-47), 2011.
16. Taksande V.K. & Kulat K.D., Simulation Comparison Among AODV, DSDV, DSR Protocol with IEEE 802.11 MAC for Grid Topology in MANET. In *2011 International Conference on Computational Intelligence and Communication Systems* (pp. 63-67), 2011.
17. Razouqi, Q., Boushehri, A., Gaballah, M., & Alsaleh, L., Combined traffic simulation scenarios performance investigation routing protocols AODV, DSR and DSDV in MANET. In *Computer Engineering Conference (ICENCO), 8th International* (pp. 74-79), 2012.
18. Yi, P. *et al.*, "A New Routing Attack in Mobile Ad Hoc Networks," *Int'l. J. Info. Tech.*, vol. 11, no. 2, 2005.

19. Adjih, H C., Raffo, D. and Muhlethaler, P. "Attacks Against OLSR: Distributed Key Management for Security," *2nd OLSR Interop/Wksp.*, Palaiseau, France, July 28–29, 2005.
20. Hu, Y-C., Perrig, A. and D. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE JSAC*, vol. 24, no. 2, Feb. 2006.
21. Gerhards-Padilla, N E., Aschenbruck, N., Martini, P., Jahnke, M., Tolle, J., *Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs*, Proceedings of the 32nd IEEE Conference on Local Computer Networks, LCN 2007, Ireland, pp. 1043-1052, 2007.
22. Agrawal, P., Ghosh, R. K. S. K. Das, Cooperative black and gray hole attacks in mobile ad hoc networks, Proceedings of the 2nd ACM international conference on Ubiquitous information management and communication, ICUIMC '08, pp.310-314. USA, 2008.
23. Marti, S. *et al.* "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6th MobiCom, Boston, MA, Aug. 2000.
24. Michiardi, P. and Molva, R. Simulation-based analysis of security exposures in mobile ad hoc networks. In Proceedings of European Wireless Conference, 2002.
25. Kaur, R., Gaur, M. S., & Laxmi, V., A novel attack model simulation in DSDV routing. In New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on (pp. 1-5), 2011.

View publication stats