International Journal of Advanced Science and Technology
Vol.115 (2018), pp.11-22
http://dx.doi.org/10.14257/ijast.2018.115.02

Effect of Black Hole Attack on the Performance of AODV Routing Protocol under Different Traffic Conditions in Mobile AdHoc Networks

Barinderpal Singh[1] and Kulbir Kaur[2]

[1]*Assistant Professor CSE Department Gian Jyoti Group of Institutions, Punjab, India*
[2]*Assistant Professor CSE Department Gian Jyoti Group of Institutions, Punjab, India*
[1]*barinderpal.singh013@gmail.com*, [2]*sbmk91@gmail.com*

Abstract

Performance of Routing protocols in MANETs degrades because of attack occur in the network. It degrades the performance by delaying the packets and refresh the routes again and again which results in less throughput. Attacks are the major challenging issue in the Mobile Adhoc Networks and disrupt the normal behaviour of routing protocols. In this paper, the Black hole attack and Rushing is introduced and the performance of AODV routing protocol is carried out with and without Black hole attack and Rushing attack under different traffic conditions with different packet sizes. The traffic conditions used in this paper is CBR which are based on TCP and UDP agents. The delay, throughput and packet delivery ratio are common measures parameters used for the comparison of performance of AODV routing protocol with and without Black hole Attack.

Keywords: *Mobile Adhoc Networks; AODV; Black hole Attack; Rushing attack; TCP; UDP; FTP; CBR; NS2; Delay; Throughput; Packet Delivery Ratio*

1. Introduction

Mobile Ad-Hoc networks are highly dynamic networks characterized by the absence of physical infrastructure [1]. An AdHoc network consists of interconnected nodes which makes a network without any fixed infrastructure and can be arranged dynamically. In recent years, the interest on adhoc networks is at their high because of the availability of wireless communication devices. The ease of deployment and the infrastructure less nature of Mobile Ad hoc Networks (MANETs) make them highly desirable for the present day multimedia communications [2]. Multiple network hops are required to deliver and exchange data across a network [3]. Capabilities and limitations are to be concerned while designing adhoc network that the physical layer imposes on the network performance. The communication links in wireless network is unreliable so it is desired to come up with an integrated design of physical, MAC and network layer [4]. Dynamic and reliable protocols are required in MANETs, as they have no infrastructure (base stations) and their network topology changes frequently [5].

From the security perspective Mobile Ad hoc Networks (MANETs) are amongst the most challenging research areas and one of the key reasons for this is the ambiguous nature of insider attacks in these networks [6]. The security threats have been extensively discussed and investigated in the wired and wireless networks [7]. MANET is highly prone to various security attacks. One of the most important categories of attack is Denial

Received (February 15, 2018), Review Result (May 5, 2018), Accepted (May 11, 2018)

ISSN: 2005-4238 IJAST

of Service (Dos) attacks [8]. Most of these attacks are targeted at disrupting the routing of control and data packets, thereby rendering MANETs insecure and unusable. [9]. There are so many attacks like Black hole attack, Rushing attack, Flooding attack, Warm hole attack, Grey hole attack etc. which effects the performance of routing protocols and degrades the performance of routing protocols when occur in the network.

The primary objective of this paper is to analyze the performance of AODV routing protocol with and without Black hole attack and Rushing attack under different traffic conditions with different packet size. The scope of this paper is to study the effect of Black hole attack and Rushing attack on the performance of AODV routing protocol. Through this paper it is find that how TCP and UDP will react under different network conditions [10]. In order to achieve this, File Transfer Protocol (FTP) [11] and Constant Bit Rate (CBR) traffic conditions is used. In this emphasized on end to end delay, throughput and packet delivery ratio. The above parameters are validating with different network size, varying number of nodes. This analysis is done to check the effect of Black hole attack and Rushing attack on the performance of AODV routing protocol under different traffic conditions with different packet size. This paper organized as a basic idea of AODV routing protocol, Black hole attack, Rushing attack, tool used, simulation and performance analyses, results, conclusion and future work.

2. AdHoc on Demand Distance Vector (AODV)

AODV is an adhoc on demand distance vector which is a type of reactive protocol. AODV is a Source drive type routing protocol [12]. In AODV the communication takes place only when desirable. In AODV a hop-to-hop methodology takes place. AODV is a combination of on demand and distance vector. On demand means the communication takes place only when needed and distance vector means a link-state protocol. In AODV a RREQ (Route Request) is send to each and every node in the network. When all intermediate nodes have a valid and appropriate route to the destination then the RREP (Route Reply) packets are sending to the source by the nodes or by the destination itself. If no valid route is finding by the nodes then the RERR (Route Error) is send to the source node.

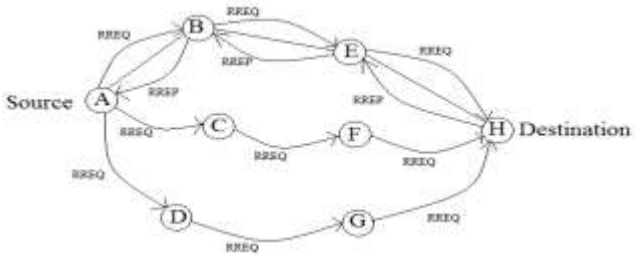


Figure 1. Working of AODV Routing Protocol

3. Black Hole Attack

A Black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors [7]. Black hole node is a malicious node which can mislead a normal node to forward the data through it and corrupt the data so that it can degrade the performance of the network [13]. Black hole degrades the performance of routing protocols when occur in the network, it results in the degradation of throughput, delay in packet delivery and deliver less packets from source to destination.

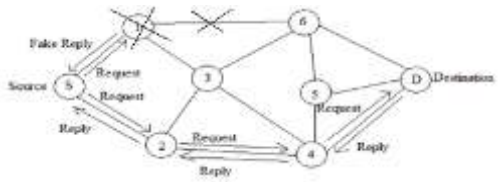


Figure 2. Black Hole Attack

4. Rushing Attack

Rushing attacks in mobile ad hoc networks (MANETs) cause system resources to become scare and isolates legitimate users from network [19]. Rushing attack degrades the performance of AODV routing protocol when occur in the network. Rushing attack is less effective denial of service attack. It is more effective when the attacker nearby source or destination node. Rushing attack is not included when there is direct communication between source node and destination node. Any MANET node can maliciously or selfishly disrupt and deny the communication of other nodes [20].

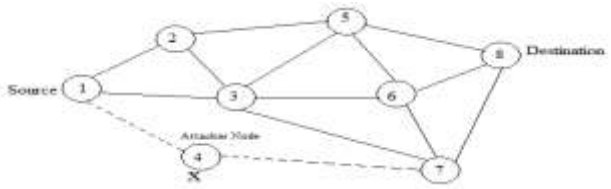


Figure 3. Rushing Attack

4. Simulation Methodology and Performance Metrics

4.1. Simulation Methodology

Performance of routing protocols is different according to their working. To analyze the performance of routing protocols simulation is done. Simulation helps in analyzing the performance of routing protocols and performance of complex networks before apply in real applications. Routing protocols suffering from many problems like Dos attacks, mobility, synchronization, localization, long route and other while routing. Therefore, these protocols should be study in depth, simulated in different conditions and classified. This classification and simulation helps in understanding, comparing performances and assist researchers to differentiate the characteristics and define the pros and cons of routing protocols [14]. The protocol whose performance is better we apply that protocol in real applications. To carry out the simulation several simulators are available which gives outputs according to the performance. In this work, the detailed study and simulation model using Network Simulator (NS-2.35) with different traffic models are presented [15] and AWK script is conducted to analyze the performance.

4.2. NS2 (Network Simulator)

NS2 is the tool which is used to carry out the performances of routing protocols of wired and wireless networks. It is a discrete event network simulator [16]. In our approach the NS2 tool is used to carry out the performances of AODV routing protocol under different parameters. NS2 is simply an event driven simulation tool that has proved useful in studying the nature of communication networks. The main components of NS2 which is used for performance analysis are: NS, Tcl/Tk, Nam, Zlib, Xgraph, Awk.

The Ns2 all in one suite can be installed in the Unix-based machine by simply running the install script and following the instructions. Firstly, we installed the NS2 and the

corresponding components and then validate which verify the essential functionalities of all installed components. In NS2 simulator several models are available in this work we consider the following models:

Node Model: Node model is for energy source, memory capacity, processing capabilities etc. Firstly, we create a new model then define it after defining validates the model and use it.

Node Deployment model: Node deployment model is for placement of nodes and its position a uniform model. The position of nodes given according to network area and movement of nodes at different speed.
Node Mobility Model: Node Mobility Model is for dynamic network topologies as Random Waypoint Mobility model. In this work Random Waypoint Mobility model is used which is a random model for the movement of nodes, and how their location, velocity and acceleration change over time.

Radio Mobile: Radio model for characteristics of radio used by node with a proper frequency, bandwidth, MAC layer functionality as IEEE 802.11 MAC model.

Wireless Signal Propagation Model: Wireless Signal Propagation model for SNIR (Signal to Noise Plus Interference Ration) at receiver as Two Ray Ground Propagation model. This model as the propagation phenomenon that results in radio signals reaching the receiving antenna.

Packet Loss Model: Packet Loss model is for packet loss or packet drop in model.

Traffic Model: Traffic is for traffic that nodes send to destination. The traffic model used in this work is CBR and UDP Model.

4.3. AWK Script

Text Processing and Data Extraction of the performance of protocols is necessary to analyze the performance of protocols and it is done by an interpreted programming language called AWK. AWK is designed for text processing and typically used as a data extraction and reporting tool [17]. AWK programs are data driven. The awk script is run according to following command:

awk –f programfile tracefile

The format of AWK script is:
BEGIN {}
{
Content
}
END {}
Begin part comprises of initialization of variable.
Commands in the content part scan every row of trace file only once.
End part having the formulation according to which data is extract from trace file.

4.4. Simulation Methods and Parameters

The goal of our experiment is to examine and analyze the effect of Black hole attack and Rushing attack on the performance of AODV routing protocol under different traffic conditions by varying number of nodes and varying network size. A major issue that affects such a network with dynamically changing topology is the performance since the nodes have both limited battery life and communicate in a bandwidth constrained network [18]. The effect of Black hole attack and Rushing attack is different under different traffic condition with different packet size is different on the performance of AODV routing protocol in MANETs.

4.5. Performance Metrics

The performance metrics helps in determining the behaviour and performance of routing protocols to achieve the quality of service (QOS). Performance Metrics measures the activities and performance of routing protocols.

End-to-End Delay: It is the time taken by the data packet to transmit across the network from source to destination. End-to-End delay depends on following components:

- *Transmission Delay (TD)*
- *Propagation Time (PT)*
- *Processing Delay (PD)*
- *Queuing Delay (QD)*

Formula of End-to-End Delay is:

End-to-End Delay = TD + PT + PD + QD.

Throughput: Throughput is the successfully data delivery over a communication network. It is the sum of the data rates that are delivered to all the terminals in a network. Formula of Throughput is:

*Throughput = received data*8/data transmission period.*

Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the source. Formula to calculate Packet Delivery Ratio is:

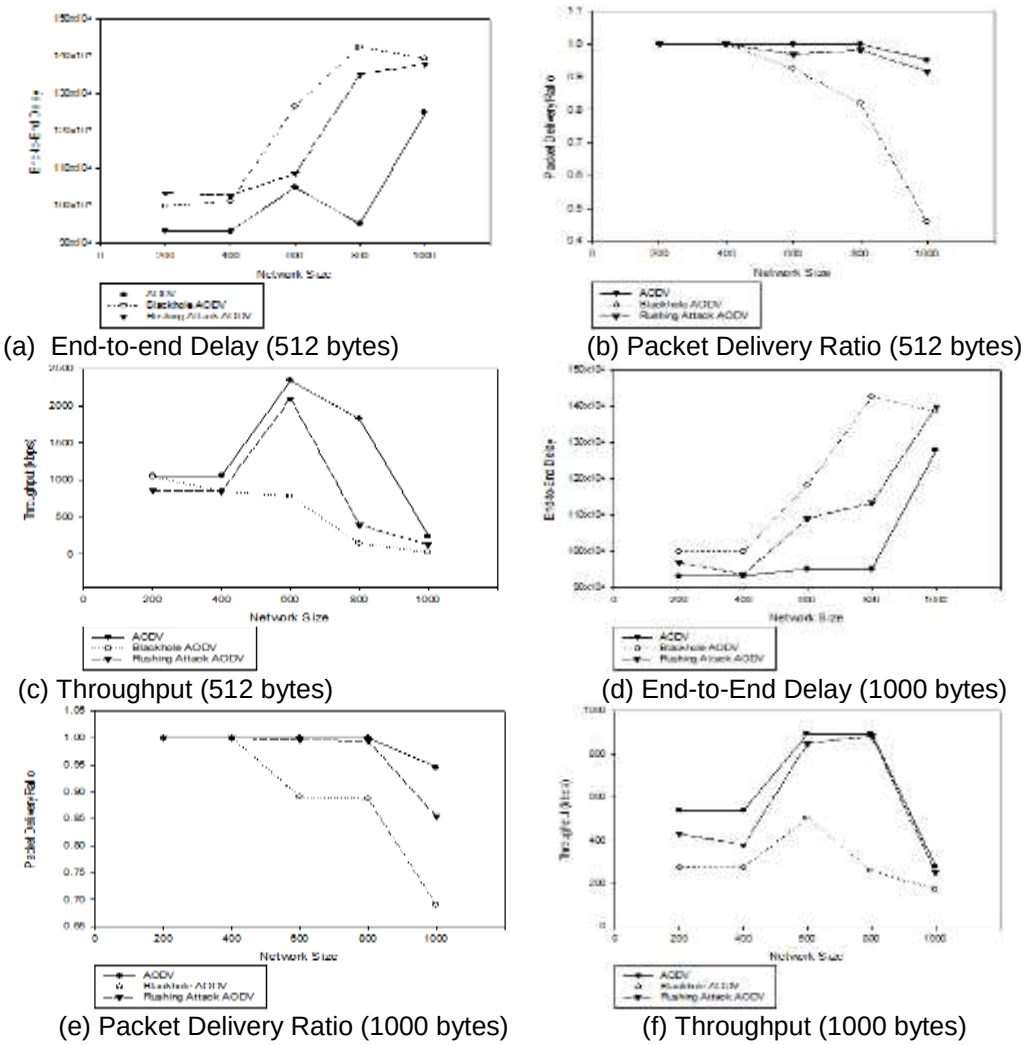
*Packet Delivery Ratio = received packets/generated packets * 100.*

5. Result Analysis of AODV Routing Protocol with and without Black Hole Attack and Rushing Attack

Table 1. Simulation Parameters and Values

SIMULATION PARAMETERS	VALUE
Channel	Wireless
Propagation Model	Two Ray Ground
Mac Address	802.11
Packet Size	512 bytes and 1000 bytes
Duration	150 sec
Routing Protocols	AODV
Attacks	Black hole Attack and Rushing Attack
Agents	TCP and UDP
Traffic Conditions	CBR
Simulation Area (sq. m)	200, 400, 600, 800, 1000
Number of nodes	10, 20, 30, 40, 50

5.1. Performance Analysis by Varying Network Size under TCP and CBR Traffic with 512 Bytes and 1000 Bytes Packet Size



(a) End-to-end Delay (512 bytes) (b) Packet Delivery Ratio (512 bytes)

(c) Throughput (512 bytes) (d) End-to-End Delay (1000 bytes)

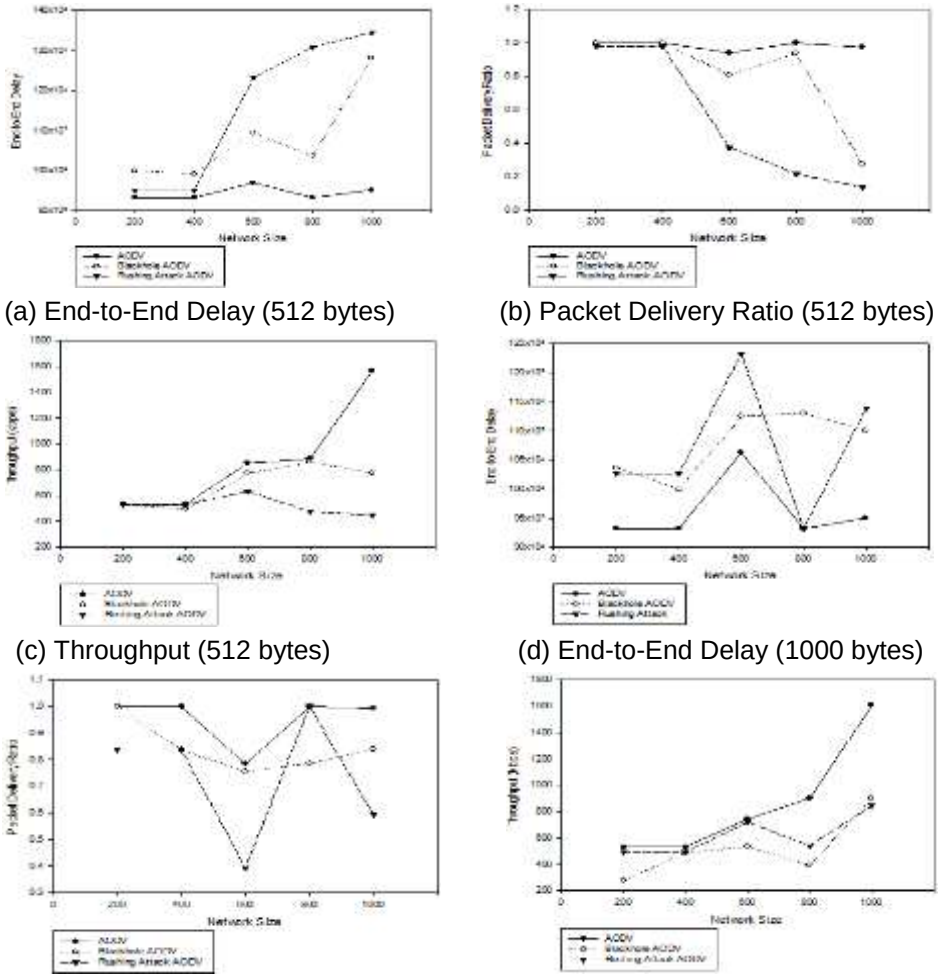
(e) Packet Delivery Ratio (1000 bytes) (f) Throughput (1000 bytes)

Figure 4. Performance Analysis under TCP and CBR Traffic by varying Network Size and Packet Size (a) Variation of End-to-end delay (512 bytes) (b) Variation of Packet Delivery Ratio (512 bytes) (c) Variation of Throughput (512 bytes) (d) Variation of End-to-end delay (1000 bytes) (e) Variation of Packet Delivery Ratio (1000 bytes) (f) Variation of Throughput (1000 bytes)

Network Size Analysis: The performance analysis of AODV routing protocol is done with and without Black hole attack and Rushing attack by varying network size *i.e.*, 200x200 sqm, 400x400 sqm, 600x600 sqm, 800x800 sqm, 1000x1000 sqm under TCP and CBR traffic condition. In Figure 4 (a) variation of end to end delay is shown with 512 bytes packet size in which delay is more when Black hole attack occur in the network and degrades the performance of AODV routing protocol whereas delay in Rushing attack is less then Black hole attack and delay in AODV protocol is less when Black hole attack and Rushing attack not occur in the network. In Figure 4 (d) the variation of delay is shown with packet size 1000 bytes. In this variation of delay with packet size 1000 bytes again the delay in Black hole effected AODV is more and Rushing attack is less but when network size is 1000x1000 sqm the delay in Rushing attack AODV is more whereas delay in normal AODV routing protocol is less when no attack occur in the network. In Figure 4 (b) variation of packet delivery ratio is shown with packet size 512 bytes. As the network

size increase the packet delivery ratio of Black hole effected AODV decreases which means it delivers less packets. Rushing attack also effect the packet delivery ratio when it occur in AODV routing protocol but its packet delivery ratio is more than Black hole attack but less than normal AODV routing protocol. In Figure 4 (e) the packet delivery ratio with 1000 bytes packet size is shown. With packet size 1000 bytes the AODV routing protocol delivers more packets without attack. Figure 4 (c) the variation of throughputs for AODV routing protocols with and without Black hole and Rushing attack is shown with packet size 512 bytes. Black hole and Rushing attack degrades the performance of AODV routing protocol which results in less throughput of AODV routing protocol than normal AODV routing protocol. In Figure 4 (f) the variation of throughput with packet size 1000 bytes is shown. AODV routing protocol gives more throughput than Black hole AODV and Rushing attack AODV. The throughput in 1000 bytes packet size is less than 512 bytes packet size.

5.2. Performance Analysis by Varying Network Size under UDP and CBR Traffic with 512 Bytes and 1000 Bytes Packet Size



(a) End-to-End Delay (512 bytes) (b) Packet Delivery Ratio (512 bytes)

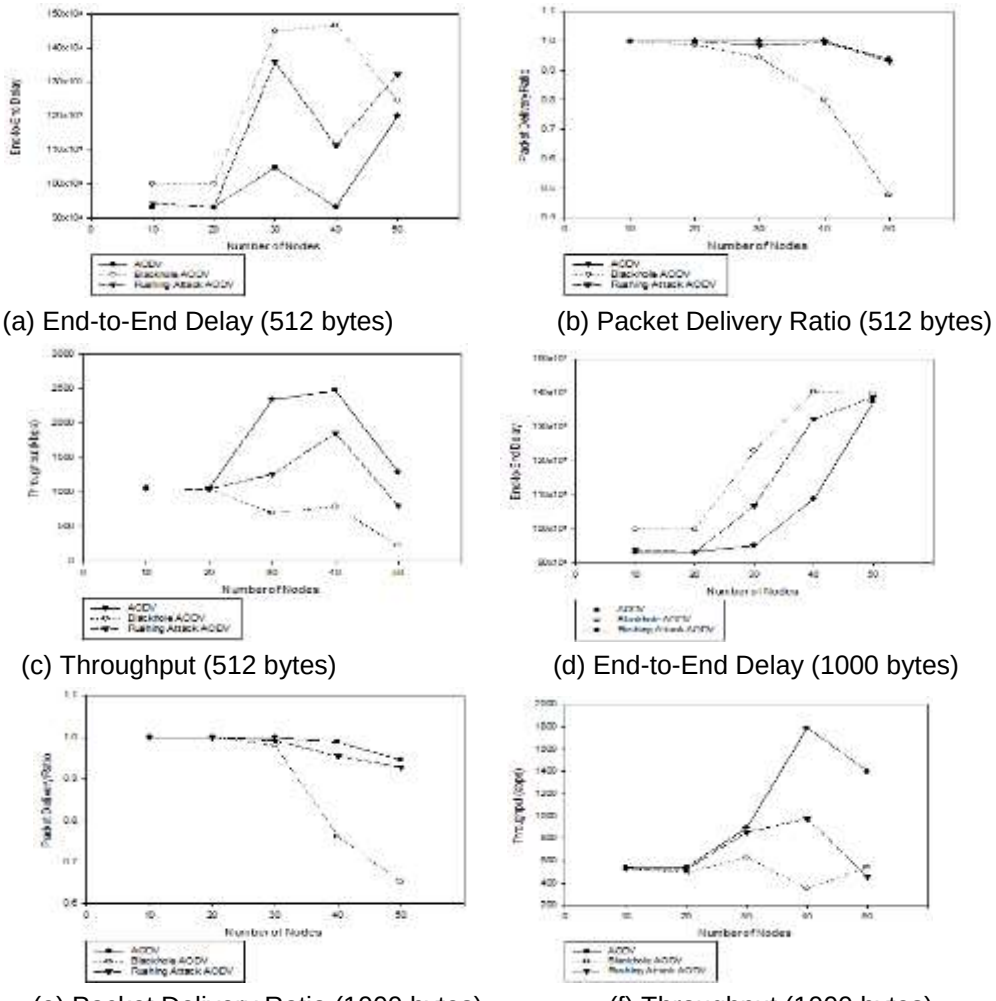
(c) Throughput (512 bytes) (d) End-to-End Delay (1000 bytes)

(e) Packet Delivery Ratio (1000 bytes) (f) Throughput (1000 bytes)

Figure 6. Performance Analysis under UDP and CBR Traffic by varying Network Size and Packet Size (a) Variation of end-to-end Delay (512 bytes) (b) Variation of Packet Delivery Ratio (512 bytes) (c) Variation of Throughput (512 bytes) (d) Variation of end-to-end Delay (1000 bytes) (e) Variation of Packet Delivery Ratio (1000 bytes) (f) Variation of Throughput (1000 bytes)

Network Size Analysis: Figure 6 shows the variation of end to end delay, packet delivery ratio and throughput is carried out with and without Black hole attack and Rushing Attack in AODV routing protocol with different packet sizes and under UDP and CBR traffic conditions. In Figure 6 (a) and 6 (d) the variation of delay is shown with packet size 512 bytes and 1000 bytes. The delay in Black hole AODV and Rushing attack AODV is more as compared to normal AODV routing protocol. In Figure 6 (b) and 6 (e) the packet delivery ratio with 512 bytes and 1000 bytes packets size is shown. The packet delivery ratio of Black hole AODV and Rushing attack AODV is less and it delivers fewer packets from source to destination. In Figure 6 (c) and 6 (f) the variation of throughput with packet size 512 bytes and 1000 bytes is shown. AODV routing protocol gives more throughput and its throughput decreases when Black hole attack and Rushing attack occur in the network.

5.3. Performance Analysis by Varying Number of Nodes under TCP and CBR Traffic with 512 Bytes and 1000 Bytes Packet Size



(a) End-to-End Delay (512 bytes) (b) Packet Delivery Ratio (512 bytes)

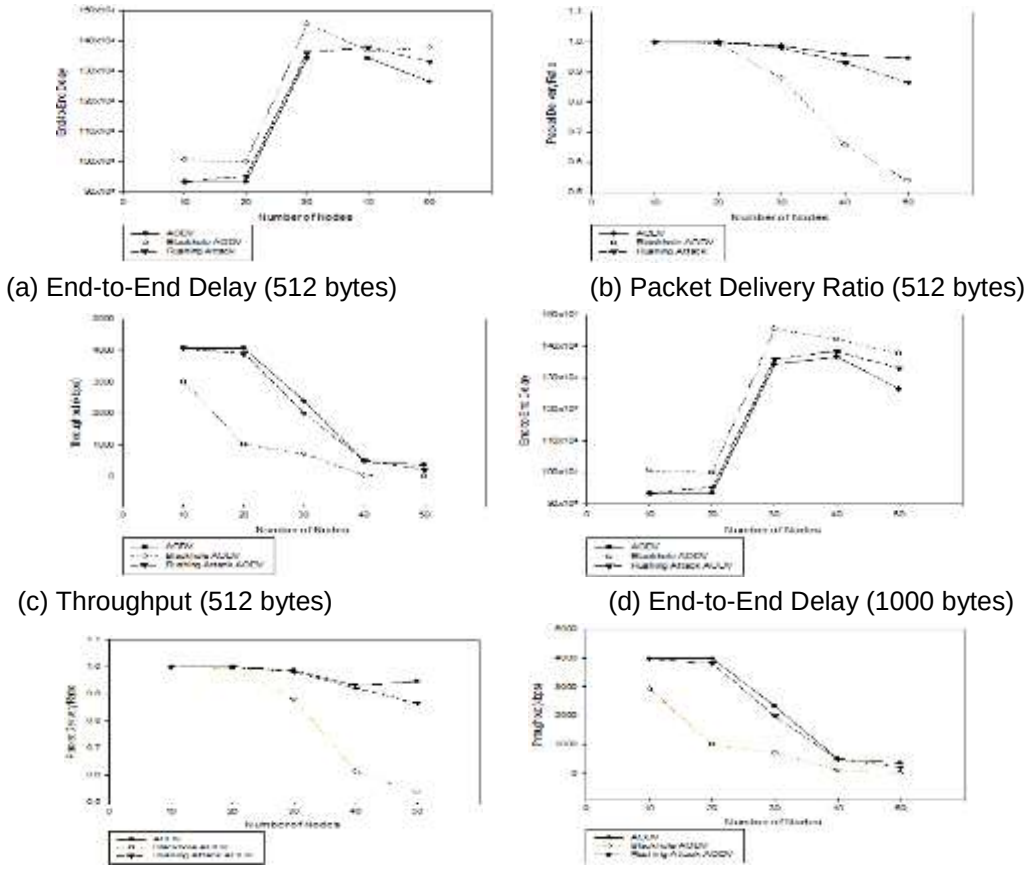
(c) Throughput (512 bytes) (d) End-to-End Delay (1000 bytes)

(e) Packet Delivery Ratio (1000 bytes) (f) Throughput (1000 bytes)

Figure 7. Performance Analysis under TCP and CBR Traffic by Varying Number of Nodes and Packet Size (a) Variation of end-to-end Delay (512 bytes) (b) Variation of Packet Delivery Ratio (512 bytes) (c) Variation of Throughput (512 bytes) (d) Variation of end-to-end Delay (1000 bytes) (e) Variation of Packet Delivery Ratio (1000 bytes) (f) Variation of Throughput (1000 bytes)

Number of Node Analysis: The performance analysis is done by varying number of nodes from 10 to 50. The number of nodes also affects the performance of routing protocols. In this the performance analysis of AODV routing protocol with and without Black hole attack and Rushing attack is carried out under different traffic conditions with different packet sizes. Figure 7 shows the performance analysis under TCP and CBR traffic by varying number of nodes with different packet sizes. In Figure 7 (a) and 7 (d) the variation of End-to-End delay is shown with packet size 512 bytes and 1000 bytes. Again the delay in Black hole AODV and Rushing attack AODV is more as compared to normal AODV routing protocol. Figure 7 (b) and 7 (e) shows the variation of Packet Delivery Ratio with packet size 512 bytes and 1000 bytes. The packet delivery ratio decreases when Black hole attack and Rushing attack occurs in the network and it delivers less packets from source to destination as compared to normal AODV routing protocol. Figure 7 (c) and Figure 7 (f) shows the variation of throughput with packet size 512 bytes and 1000 bytes. Black hole attack and Rushing attack degrades the performance of AODV routing protocol which result in less throughput. Black hole attack is more effective then Rushing attack.

5.4. Performance Analysis by Varying Number of Nodes under TCP and FTP Traffic with 512 Bytes and 1000 Bytes Packet Size



(a) End-to-End Delay (512 bytes) (b) Packet Delivery Ratio (512 bytes)

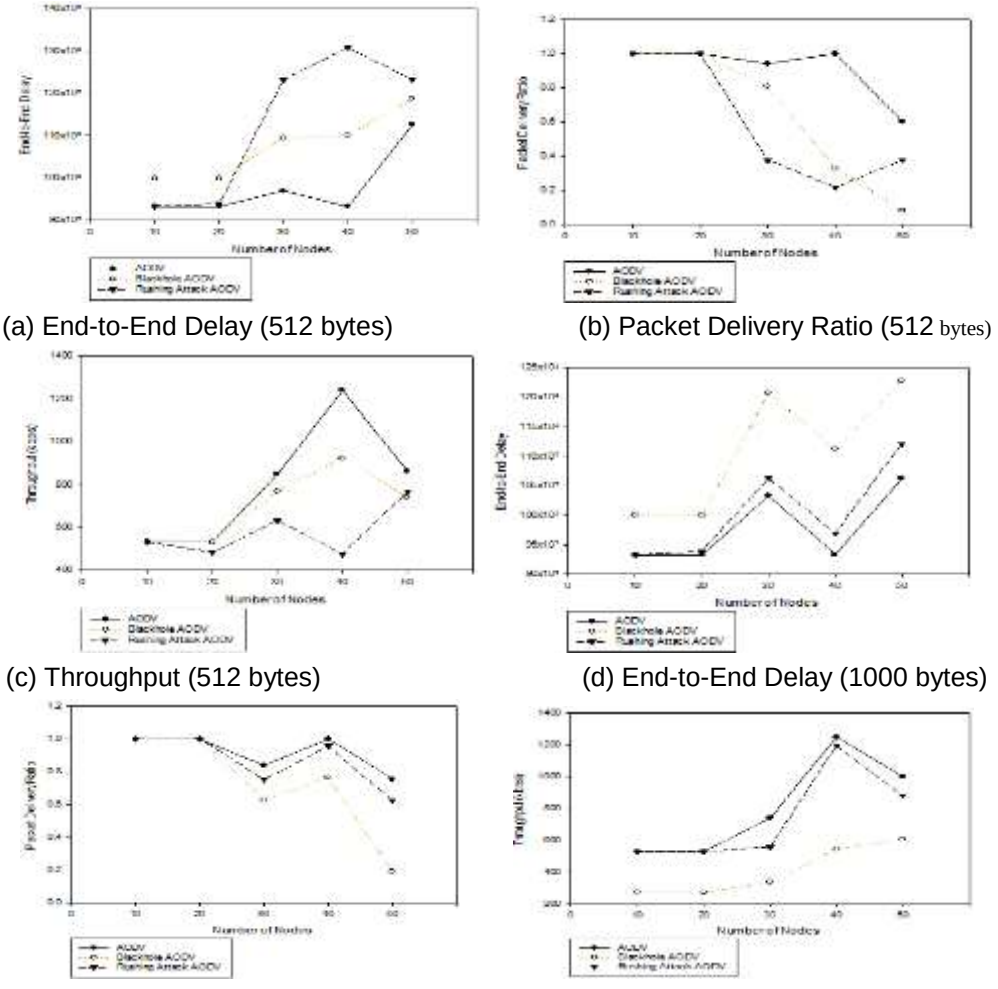
(c) Throughput (512 bytes) (d) End-to-End Delay (1000 bytes)

(e) Packet Delivery Ratio (1000 bytes) (f) Throughput (1000 bytes)

Figure 8. Performance Analysis under TCP and FTP traffic by Varying Number of Nodes and Packet Size (a) Variation of end-to-end Delay (512 bytes) (b) Variation of Packet Delivery Ratio (512 bytes) (c) Variation of Throughput (512 bytes) (d) Variation of end-to-end Delay (1000 bytes) (e) Variation of Packet Delivery Ratio (1000 bytes) (f) Variation of Throughput (1000 bytes)

Number of Node Analysis: Figure 8 shows the performance analysis of AODV, Black hole AODV and Rushing attack AODV routing protocol under TCP and FTP traffic by varying number of nodes with different packet sizes. In Figure 8 (a) and Figure 8 (d) the variation of End-to-End Delay is shown with packet size 512 bytes and 1000 bytes. The delay is more in Black hole AODV and Rushing attack AODV as compared to normal AODV. Black hole attack and Rushing attack effected AODV delay the packets which are send form source to destination. Figure 8 (b) and Figure 8 (e) shows the variation of Packet Delivery Ratio with packet size 512 bytes and 1000 bytes. The AODV routing protocol delivers more packets and when Black hole attack and Rushing attack occur in the network it delivers less packets and its packet delivery ratio become low. In Figure 8 (c) and 8 (f) the variation of throughput with packet size 512 bytes and 1000 bytes is shown. The throughput of AODV routing protocol is more and its throughput degrades when Black hole attack and Rushing attack occur in the network.

5.6. Performance Analysis by Varying Number of Nodes under UDP and CBR Traffic with 512 Bytes and 1000 Bytes Packet Size



(a) End-to-End Delay (512 bytes) (b) Packet Delivery Ratio (512 bytes)

(c) Throughput (512 bytes) (d) End-to-End Delay (1000 bytes)

(e) Packet Delivery Ratio (1000 bytes) (f) Throughput (1000 bytes)

Figure 9. Performance analysis under UDP and CBR Traffic by Varying Number of Nodes and Packet Size (a) Variation of end-to-end Delay (512 bytes) (b) Variation of Packet Delivery Ratio (512 bytes) (c) Variation of Throughput (512 bytes) (d) Variation of end-to-end Delay (1000 bytes) (e) Variation of Packet Delivery Ratio (1000 bytes) (f) Variation of Throughput (1000 bytes)

Number of Node Analysis: Figure 9 shows the performance analysis of AODV routing protocols with and without Black hole attack and Rushing attack under UDP and CBR traffic condition by varying number of nodes and packet size. Figure 9 (a) and Figure 9 (d) shows the variation of End-to-End Delay with packet size 512 bytes and 1000 bytes. In 512 bytes packet size the delay is more when Rushing attack occur in the network and Black hole attack have less effect when packet size is 512 bytes. In packet size 1000 bytes the delay is more when Black hole attack occurs in the network and the delay without attack is less. Figure 9 (b) and Figure 9 (e) shows the variation of Packet Delivery Ratio with packet size 512 bytes and 1000 bytes. The packet delivery ratio of AODV routing protocol is more as compared to Black hole AODV and Rushing attack AODV. Without attack the AODV routing protocol delivers more packets from source to destination. Figure 9 (c) and 9 (f) shows the variation of throughput with packet size 512 bytes and 1000 bytes. Black hole attack and Rushing attack affects the performance of AODV routing protocol which results in less throughput as compared to normal AODV routing protocol.

6. Conclusion

In this paper the performance analysis of AODV routing protocol is carried out under two denial of service attacks i.e. Black hole attack. The performance analysis is carried out by varying network size and number of nodes under each traffic condition with 512 and 1000 bytes packet size. The three measuring parameters i.e. End-to-End Delay, Packet Delivery Ratio and Throughput are used to analyze the performance of routing protocol. Black hole attack degrades the performance of AODV routing protocol which results in more delay in packets, less packet delivery ratio which means it delivers less packets from source to destination and less throughput. Black hole attack disrupt the performance of AODV routing protocol when occur in the network. The Black hole affected node sends fake reply to source and do not forward the packets which results in degradation of performance of AODV routing protocol. The data packet size also affects the performance of routing protocol as the packet size increases the throughput decreases. The protocol performs different under FTP and CBR traffic conditions. It affects the quality of service of routing protocol. In future, prevention methods are applied which prevents the Black hole attack and Rushing attack to be occur in the network. This will increases the quality of service of AODV routing protocol.

References

[1] A Tuteja, A Gujral and A Thalia, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2", IEEE Comp. Society, **(2010)**, pp. 330-333.
[2] A. Bagwari, R. Jee, P. Joshi, S. Bisht, "Performance of AODV Routing Protocol with Increasing the MANET Nodes and its Effects on QOS of Mobile Ad Hoc Networks", IEEE, International Conference on Communication Systems and Network Technologies (CSNT), **(2012)** May.
[3] R. Desai and B. P. Patil, "Analysis of routing protocols for Ad Hoc Networks", IEEE, Communication and Information Technology Applications (CSCITA), **(2014)**.
[4] S. Mohapatra and P. Kanungo, "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator", International Conference on Communication Technology and System Design, **(2011)**.
[5] N. Sharma, S. Rana and R. M. Sharma, "Provisioning of Quality of Service in MANETs performance analysis & comparison (AODV and DSR)", IEEE, 2nd International Conference on Computer Engineering and Technology (ICCET), **(2010)**.
[6] H. Ehsan and F. A. Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs", IEEE, 11th International Conference on Trust, Security and Privacy in Computing and Communication (TrustCom), **(2012)**.
[7] F.-H. Tseng, L.-D. Chou and H.-C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Springer, Human-centric Computing and Information Sciences, **(2011)**.
[8] A. D. Patel and K. Chawda, "Blackhole and grayhole attacks in MANET", IEEE, International Conference on Information Communication and Embedded Systems (ICICES), **(2014)**.

[9] K. Das and A. Taggu, "A comprehensive analysis of DoS attacks in Mobile Adhoc Networks", IEEE, International Conference on Advances in Computing, Communications and Informatics (ICACCI), **(2014)**.
[10] M. S. Chaudhary and V. Singh, "Simulation and Analysis of Routing Protocol under CBR and TCP Traffic Source", IEEE, Communication Systems and Network Technologies (CSNT), **(2012)**.
[11] D. Kampitaki and A. A. Economides, "Simulation study of MANET routing protocols under FTP traffic", ELSEVIER, Conference on Electronics, Telecommunications and Computers-CETC, **(2013)**.
[12] S. Liu, Y. Yang and W. Wang, "Research of AODV Routing Protocol for Ad Hoc Networks", ELSEVIER, AASRI Conference on Parallel and Distributed Computing and Systems, **(2013)**.
[13] S. Jalal Ahmed, V. S. Reddy, A. Damodaram and P. Radha Krishna, "Detection of Black Hole Attack Using Code Division Security Method", Springer, Advances in Intelligent Systems and Computing, vol. 338, **(2015)**.
[14] S. El Khediri, N. Nasri, A. Benfradj, A. Kachouri and A. Wei, "Routing protocols in MANET: Performance comparison of AODV, DSR and DSDV protocols using NS2", IEEE, International Symposium on Networks, Computers and Communication, **(2014)** June.
[15] S. El Khediri, N. Nasri, A. Benfradj and A. Kachouri, "Routing protocols in MANET: Performance comparison of AODV, DSR and DSDV protocols using NS2", Networks, IEEE, International Symposium on Computers and Communications, **(2014)** June.
[16] P. Rajankumar, P. Nimisha and P. Kamboj, "A Comparative study and simulation of AODV MANET routing protocol in NS2 & NS3", IEEE, International Conference on Computing for Sustainable Global Development (INDIAcom), **(2014)** March.
[17] A. D. Robins, "GAWK:an effective AWK programming", 3rd ed, **(2010)** April.
[18] Q. Razouqi, M. Gaballah and L. Alsaleh, "Combined traffic simulation scenarios performance investigation routing protocols AODV, DSR and DSDV in MANET", IEEE, 8th International Conference on Computer Engineering (ICENCO), **(2012)**.
[19] A. S. Al Shahrani, "Rushing Attack in Mobile Ad Hoc Networks", IEEE, Third International Conference on Intelligent Networking and Collaborative Systems (INCoS), 2011.
[20] A. Rawat, P. D. Vyavahare and A. K. Ramani, "Evaluation of rushing attack on secured message transmission (SMT/SRP) protocol for mobile ad-hoc networks", IEEE, International Conference on Personal Wireless Communications, **(2005)**.

