International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 11 (2015) pp. 29581-29594

http://www.ripublication.com

PERFORMANCE ANALYSIS OF AOMDV UNDER THE IMPACT OF RUSHING ATTACK

V. Muthupriya and K. M. Mehata
muthupriya@bsauniv.ac.in, kmmehata@bsauniv.ac.in
Department of Computer Science and Engineering,
B. S. Abdur Rahman University, Seethakathi Estate,
GST Road, Vandalur, Chennai –6000 48, India.
Mobile no: 9841862224, Mail-id: muthupriya@bsauniv.ac.in

Abstract

MANETS are mostly susceptible to various routing attacks due to its open access wireless medium. Several On-demand routing protocols have been designed to enable routing in MANET e.g. AODV, DSR, etc. The AOMDV is the enhanced AODV where in multipath is discovered to minimize the delay in data packet transmission. Most of the research works for reducing the routing attacks were carried out in on-demand routing protocols, but less attention was given on AOMDV. In this paper the impact of a rushing attack in AOMDV routing protocol is analyzed and its results were compared to a black hole in order to prove that the rushing attack is more significant than other routing attack. The overall performance of the AOMDV under the impact of rushing attack and black hole attack is studied using the NS2 simulator by calculating its packet delivery ratio, throughput, routing overhead and average end-to-end delay.

Keywords: MANET, AODV, AOMDV, Rushing attack, Black hole attack.

Introduction

The MANET [1] is a group of wireless nodes, which are dynamic, infrastructure less and uses unguided medium for data transmission. Since they don't have a fixed network topology they lack centralized control. The main applications of this type of networks are in dynamic business meetings, mining operations, robot data acquisition, rescue operations in battlefields and during times of natural disasters.

The main services rendered by a network layer protocol for any type of network are route establishment and congestion control. In MANET mobile network layer is responsible for packet delivery between source and destination. Since there is no

dedicated node in a MANET to perform packet forwarding or for network management it uses available nodes to do these tasks. The major issues in ad hoc networks concerned to routing are mobility, bandwidth constraint, error prone and shared channel, resource constraints and insecure hop-to-hop data transmission. This enforces several security mechanisms in the network to ensure reliable packet delivery in the network.

The routing in MANET is classified as either proactive (Table-driven) or reactive (On-demand). In proactive routing, all the nodes maintain the network status of their neighbour nodes by exchanging it for every defined time interval. Thus, by using this information, the routing path between the source and destination is predetermined and available in the routing table. Due to exchange of control packets in the network there will be increase of network overhead in proactive routing. In reactive routing the routing path between the source and destination is founded only during the time of transmission. This is done by initially forwarding Route Request (RREQ) packet in the network. Ad hoc On Demand Vector Routing (AODV) and Dynamic Source Routing (DSR) [3] are the common on-demand routing protocols used for routing in MANET.

The routing can be categorized as a single path and multipath routing depending on the number of paths discovered during the route discovery phase. Multipath routing is comparatively reliable and secure because if there is any link breakage due to any attack or resource depletion in nodes, it can take alternate path for data transmission. DSR is basically a multipath routing protocol where as AODV [4] is a single path routing protocol. The possible routing attacks in on demand routing protocol [7] are worm hole attack, black hole attack, Byzantine attack, flooding attack, gray hole attack, rushing attack, spoofing attacks, etc. In this paper simulation study of rushing attack in AOMDV is analysed and is results are summarized.

Ad Hoc On Demand Vector (AODV)

In AODV [2] according to the requirement of the source, a single path is discovered between source and destination by flooding the RREQ packets via intermediate nodes. The two main phases of AODV protocol are route discovery and route maintenance phase.

Route Discovery Phase

In MANET when any node wants to have a data transmission it will broadcast a Route Request (RREQ) packet to its neighboring nodes. The RREQ packet contains following information,

- Source address
- Source sequence
- Broadcast id
- Destination address
- Destination sequence
- Hop count

The source address and broadcast id together form a RREQ identification to prevent the loop formation in the route and also avoids intermediate nodes to accept RREQ with the same identification. This process is called duplicate suppression of the RREQ. If the RREQ reaches the destination node, it stops forwarding RREQ. If the RREQ is received for the first time either at destination node or at intermediate node and if there is no new route to the destination from intermediate node, it will immediately send a route reply (RREP) to the sender to confirm the path to the sender. Also forward pointer is maintained between the source and destination along the path from where the RREP is originated. The RREP packet contains following information,

- Source address
- Destination address
- Destination sequence
- Hop count
- Lifetime

A node (including destination node) on receiving RREP propagates towards source only if it is received for first time otherwise it checks for the destination sequence number. The RREP is propagated only if the destination sequence number is greater than that of previous RREP's destination sequence number otherwise discarded. In case of new route it is accepted by the node only if the destination sequence number of new routes is greater than the destination sequence number of older routes. If both are equal it checks for the hop count and accepts the new route only if the hop count is lesser than the old route.

Route Maintenance Phase

The Route Error (RERR) message is sent to the sender by the intermediate node if there is any link breakage between itself and sender. This interrupts the data transmission till it finds the available alternate path otherwise it repeats the route discovery phase to establish a new path. This will avoid loss of data during transmission. Since for every link failure the route has been rediscovered it induces more delay in AODV protocol.

Ad Hoc On Demand Multipath Vector (AOMDV) [5, 6]

AOMDV an extension of AODV is proposed by Mahesh et al [10], which is intended to reduce packet loss by up to 40% and achieves a remarkable improvement in the end-to-end delay. In this multiple paths are discovered between the source and destination which enables reliable transmission at the times of link breakage. Multiple paths are guaranteed to be loop-free and disjoint. Like AODV it also has two phases route discovery and route maintenance phase.

Route Discovery Phase

In route discovery phase the protocol aims to find node disjoint and link disjoint multipath. The node disjoint multipath is where no routing path will have a common node, whereas in link disjoint multipath, a node can be in common but no link is

common in alternate paths. The node disjoint paths are more reliable than link disjoint as the link breakage due to loss of energy in any particular node is less.

The route discovery phase in AOMDV is also initiated by broadcasting the RREQ from the source. Unlike AODV the neighbor nodes and destination nodes will accept duplicate RREQs and send multiple RREPs to sender node. Though the protocol sends multiple RREPs it follows AOMDV route update rule [6] for finding loop free and disjoint routes between any sender and receiver nodes.

Route Maintenance Phase

The route maintenance phase is similar to AODV where an intermediate node generates and forwards RERR towards upstream nodes whenever there is a link failure. Unlike AODV alternate routes are available and so it transmits the packets without much delay. When all the alternate paths are exhausted a new route discovery phase is initiated. The main advantage of AOMDV is, it reduces overall end to end delay during the period of link breakage by resuming the process with alternate paths.

Rushing Attack [9]

Rushing attack is a DOS attack which attacks the routing path easily and makes itself as a one of the communicating nodes unnoticeable to other nodes. In rushing attack the attacker gets easily included in the routing path by quickly forwarding the RREQ packet without any delay. Due to duplicate suppression nature of routing protocols the RREQ from rushing attacker reach the destination quicker than from other nodes.

The Figure 4.1 is actually showing a wireless network where the edges are used to represent the bidirectional connection between the nodes under same transmission range. In this S is the source node and D is the destination node, the neighbour nodes are connected through one hop edge. Whenever S wants to send a data to D it initially, forwards a RREQ packet to its neighbors A, B, M. In any wireless networks, there will be a delay in any node before forwarding the RREQ packet due to following reasons.

- The nodes whenever receive any RREQ packet usually check for the uniqueness of the RREQ by verifying the source address and broadcast id. In most of the routing protocols like AODV the same RREQ received for the second time will be discarded.
- Also, it verifies whether the path to the demanded destination is already available, if so, it sends the path information back to the sending node otherwise broadcasts the RREQ to its neighbor nodes.

In this case M is a rushing node where on receiving the route request unlike other nodes will broadcast the route request packet to its neighbors immediately without any delay. Since the route request from M reaches C earlier than from B, because of the duplicate suppression nature of the protocol the route request from B is discarded in C. Hence the destination node forwards the route reply through node M to the source and gets included in the routing path. This makes the attacker node to easily get into the access path and take a control over the whole network.

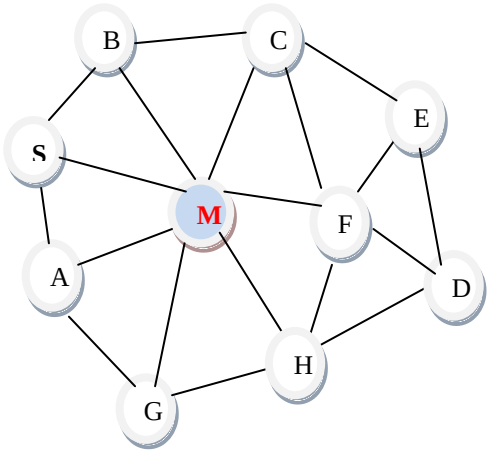

Figure 4.1: Network with Rushing Attack

The rushing attack can be exhibited in any of the three places i.e., near source, near destination or in intermediate between source and destination.

Impact of Rushing Attack in AOMDV

The AOMDV unlike AODV does not possess duplicate suppression nature, they generate loop free disjoint multipath. In this paper, rushing attack in AOMDV is focused, where number of routes discovered at route discovery phase is reduced due to this attack. Whenever there is route drop in a AOMDV during transmission time, it searches for available alternate route and forwards the packet through it. Since number of available alternate path is considerably very less due to rushing attack, the protocol need to discover new routes when the available routes are exhausted. This causes increase in end-to-end delay in the network. Due to increase in end-to-end delay the throughput of AOMDV protocol decreases.

In the Figure 4.1 consider M as a normal node and the node S sends a route request to node D. The AOMDV protocol finds SMFD, SAGHD, SBCED are the possible disjoint paths between S and D during the route discovery phase. All three paths formed are links disjoint as well as node disjoint and so they are very much reliable for packet transmission with less delay.

Once the node M becomes a compromising node and exhibit rushing node behaviour the number of disjoint paths formed between the source and destination will get reduced. The M as a rushing node, will forward the RREQ quickly without any delay to its neighbour nodes. So the node C receives a RREQ from M earlier than

from B. Similarly, node G receives RREQ earlier from M than from A. So there is a possibility of routing path SMFD, SMCED than SBCED and SMGHD or SMHD than SAGHD. The number of link disjoint paths and node disjoint paths are three and one respectively. This indicates that there is an inclusion of a node M in most of the paths founded during the route discovery phase. So the number of node disjoint paths generated by the protocol AOMDV will get reduced. This shows by imposing rushing node M in the network (Figure 4.1) it will reduce the overall disjoint paths formed by AOMDV. As said previously due to decrease in path the end to end delay increases. This causes throughput depreciation and thus the performance of the protocol in the network is affected.

Related Work

Yih-Chun Hu et.al [9] proposed the mechanisms such as secure neighbor detection, secure route delegation and randomized Route Request forwarding to reduce rushing attack. Latha.T, and Sankaranarayanan.V [8], in their research work have given a solution to prevent a rushing attack. After receiving the RREQ the every node will wait for some amount of time and store the all the RREQ received through other nodes. In this it avoids forwarding the first route request packet received from neighbors and randomly sends the RREQ from the stored list. So that rushing attack could be prevented from the routing path. Cross-Layer Intrusion Detection System (CLIDS) [11] is proposed to overcome rushing attack. It uses behavioral information like packet drop ratio, channel rate from MAC layer and hop count from the network layer for the detection. Sathyam Shrivastava [10] proposed a scheme based on the transmission time a threshold value is fixed and on verifying this the RREQ is either accepted or discarded. Gajendra Singh Chandel and Rajul Chowksi, [12] have fixed a threshold value with reference to request rate and accordingly RREQ is either accepted or discarded.

In most of the research works carried out till now the impact of rushing attack in AODV and DSR are majorly discussed. Also, they sometimes provide multipath protocol like AOMDV as a solution for routing attack. So that it finds an alternate path when there is an inclusion of any routing attack in the path. The rushing attack will have its impact during route discovery phase itself, while other routing attacks show its impact only during transmission time. Since rushing attack reduces the number of routes discovered in multipath protocols, these protocols cannot be used as a solution for rushing attack. In this paper one such protocol AOMDV is taken into consideration and its parameters were analysed in the presence of rushing attack.

Comparison of Rushing Attack with other Routing Attack in AOMDV

The on demand routing protocols are more prone to routing attacks [7]. Many research works on such attacks, namely the Black hole, Wormhole, Gray hole, Route cache poisoning, Flooding attack, Replay attacks, Jelly fish attacks were carried out and several solutions were proposed. Mostly these works focus on routing protocols

like AODV and DSR and lesser attention is given on AOMDV. Since AOMDV is more reliable than AODV at the times of link breakage, it must ensure that all the alternate paths are secure for data transmission without any routing attacks. In this paper, we analyse the reason for performance degradation in AOMDV due to Rushing attack. It is a more serious attack because this attack paves way for above said all other routing attacks. By becoming a rushing attacker node, the node can easily enter into the routing path and exhibit following characteristics.

- It can easily drop the data packets forwarded through it.
- It may cause some delay in transmitting the packet.
- It may play, replay attack in order to exhaust energy of the nodes in the network.
- Selective drops of packets.
- Disrupt the communication and enforce Denial of Service (DOS) attacks in the network.

In this paper the performance metrics of AOMDV under the impact of rushing attack is analyzed and its results were compared with AOMDV under black hole attack. The result shows the black hole attack doesn't show much variation in throughput, packet delivery ratio and average end to end delay whereas the rushing attack affects these parameters very much.

Simulation Study

Performance Metrics

The comparison on the following metrics over AODV and AOMDV were analyzed using NS2 Simulator.

- **Average End-to-End delay:** The time taken from the packet to reach the destination from the source. It includes all buffering delays, retransmission delays and propagation delays.
- **Packet Delivery ratio**: The ratio of number of packets received over number packets transmitted.
- **Throughput:** It is the measure of the average number of bits transmitted per second.
- **Route Drop:** The number of times the route gets dropped due to link failure in the network.

Simulation Environment

The performance was analysed for the following simulation Parameters using NS2.

Table 5.1: NS2 Simulation Parameters

Parameter Type	**Value**
Simulator	NS 2.35
Channel Type	Wireless
Propagation model	TwoRayGround
Mobility Model	Random way point
Network interface type(netif)	Phy/WirelessPhy
MAC type(mac)	802.11
Interface queue type (ifq)	DropTail/PriQueue
Maximum speed	20 m/s
Antenna model	Omni Antenna
Max packet in ifq	50
Number of mobile nodes	100
Routing protocol	AODV, AOMDV
Simulation time	200sec
X&Y dimension of topology	1000 m, 1000m
Traffic Source	CBR
CBR packet size	512 bytes
CBR packet rate	10 packets/s
Transmission range	250m
Pause Time	10,20,30,40,50,60,70,80,90,100

Result and Analysis

The simulation study was carried out based on the given NS2 simulation parameters in the Table 5.1.In this out of 100 nodes 6 nodes near source, 6 nodes near destination and 6 intermediate nodes i.e., On the whole 18 nodes are set as rushing attacker nodes. The AOMDV performance metrics packet delivery, throughput, average end to end delay, number of route drops under the impact of rushing attack and black hole attack are analyzed and summarized in the Table 5.3, Table 5.4, Table 5.5, and Table 5.6.

The AOMDV under the impact of rushing attacker node is represented as AOMDV_rus and black hole attack as AOMDV_black. The AOMDV_rus is compared with AODV and AOMDV, AOMDV_black and graphical representations are given in the Figure 5.1, Figure 5.2, Figure 5.3 and Figure 5.4. Usually when we compare AOMDV with AODV the overall end to end delay (Figure 5.4) of AOMDV will be less due to multipath available during the time of link failure. So the impact of rushing attack (AOMDV_rus) in AOMDV is studied and comparative analysis is made with AODV, AOMDV and AOMDV_black in order to show that the overall end to end delay in AOMDV_rus increases even more than that of AODV.

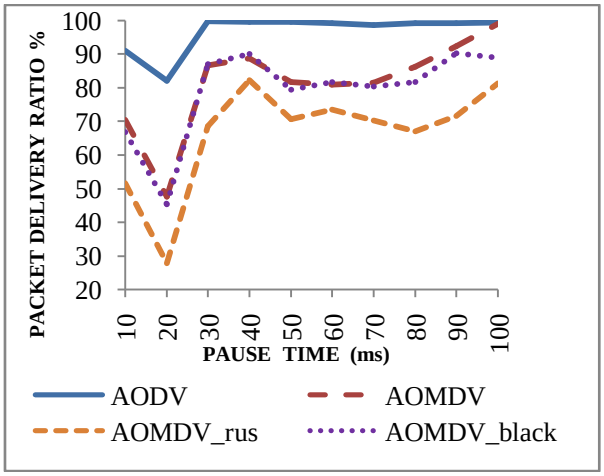

Figure 5.1: Packet Delivery Ratio (PDR) Vs. Pause Time

The result also shows that the impact of the black hole attack in AOMDV (AOMDV_black) does not show much significant change in AOMDV performance when compared to AOMDV_rus.

Table 5.2: Packet Delivery Ratio (PDR) Vs. Pause Time

PAUSE TIME (ms)	**PACKET DELIVERY RATIO %**			
	AODV	**AODMV**	**AOMDV_ rus**	**AOMDV_black**
10	91.01	70.59	51.65	66.88
20	82.07	47.64	27.8	45.29
30	99.8	86.75	68.65	87.15
40	99.74	88.77	82.38	90.15
50	99.65	81.69	70.76	79.4
60	99.29	80.93	73.5	81.77
70	98.64	81.63	70.32	80.48
80	99.25	86.41	67.05	81.74
90	99.24	92.34	71.60	90.4
100	99.54	99.01	81.41	89

The figure 5.1 and table 5.2 shows the comparison of the packet delivery ratio between AODV, AOMDV, AOMDV_black and AOMDV_rus. The graph is not linear since the mobility of the nodes depends on various parameters like pause time, number of nodes, distance between the source and destination, maximum speed, etc.

In this simulation all the other parameters except pause time are fixed. By varying the pause time when we compare the packet delivery ratio of AOMDV_rus with AODV, AOMDV and AOMDV_black there is more packet loss in AOMDV_rus. Though the packet delivery ratio is high for AODV at the lesser pause time the end-

to-end delay is very much higher for AODV than AOMDV. Also, it shows the AOMDV_black does not affect the packet delivery ratio much in AOMDV.

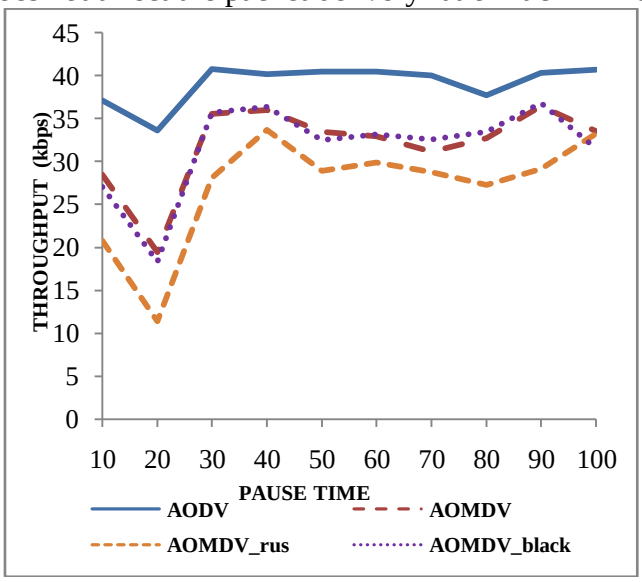

Figure 5.2: Throughput Vs. Pause Time

The figure 5.2 and table 5.3 shows for the same pause time, when compared with AODV, AOMDV and AOMDV_black the throughput of AOMDV_rus is very much less. The number of bits transmitted for 200ms is reduced due to increase in route drop in AOMDV_rus. This can be seen in the figure 5.3 and table 5.4.

Table 5.3: Throughput Vs. Pause Time

PAUSE TIME (ms)	**THROUGHPUT (kbps)**			
	AODV	**AODMV**	**AOMDV_ rus**	**AOMDV_ black**
10	37.11	28.47	20.83	27.05
20	33.57	19.46	11.39	18.35
30	40.8	35.53	28.12	35.7
40	40.16	35.94	33.71	36.37
50	40.53	33.44	28.9	32.52
60	40.47	32.9	29.92	33.16
70	40.08	31.11	28.77	32.58
80	37.72	33.52	27.3	33.46
90	40.37	38.46	29.12	36.82
100	40.69	40.31	33.28	31.56

This route drop occurs several times in AOMDV_rus because the number of alternate disjoint paths discovered during the route discovery phase is less when the pause time is less. As the pause time increases, though the route drop decreases in

AOMDV_rus but it is comparatively lesser than AODV, AOMDV and AOMDV_black.

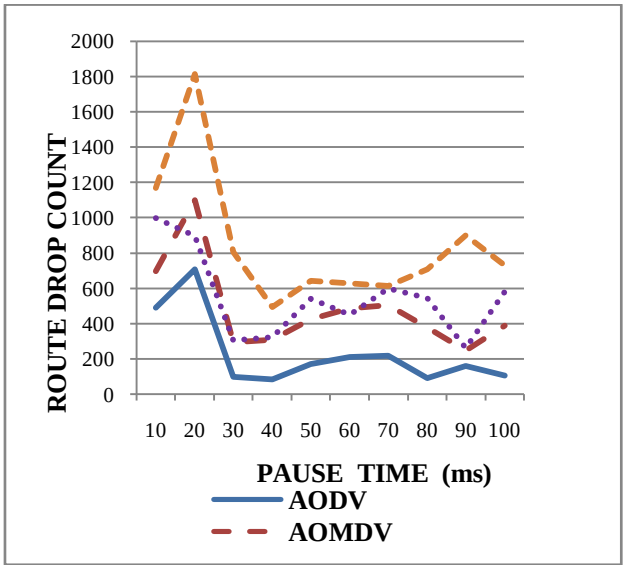

Figure 5.3: Route Drop Count Vs Pause Time

Table 5.4: Route Drop Count Vs. Pause Time

PAUSE TIME (ms)	ROUTE DROP COUNT (no's)			
	AODV	AODMV	AOMDV_rus	AOMDV_black
10	37.11	28.47	1169	998
20	33.57	19.46	1814	896
30	40.8	35.53	807	306
40	40.16	35.94	496	321
50	40.53	33.44	643	539
60	40.47	32.9	630	448
70	40.08	31.11	616	600
80	37.72	33.52	710	545
90	40.37	38.46	902	261
100	40.69	40.31	730	580

Similarly, when we analyze the average end-to-end delay in figure 5.4 and table 5.5 in AOMDV_rus it is very much higher when compared to AODV, AOMDV and AOMDV_black. When we normally compare AOMDV with AODV, the packet delivery ratio is comparatively low, but as the pause time increases the AOMDV shows far better performance [13]. This is because it finds more alternate disjoint paths when the pause time is more which can be effectively used during the time of link breakage. In AOMDV_rus due to rushing attacker node the number of alternate disjoint path generated by the AOMDV protocol reduces and thus the routing overhead increases. So at the time of link breakage the delay is increased for finding

the alternate path for data transmission. Thus we finally conclude from the above simulations that the overall performance of AOMDV degrades when there is an impact of rushing node in the network.

Also the figure-5.4 depicts the comparison between rushing attack and black hole attack in AOMDV. The average end to end delay is very badly increased under rushing attack than under black hole attack.

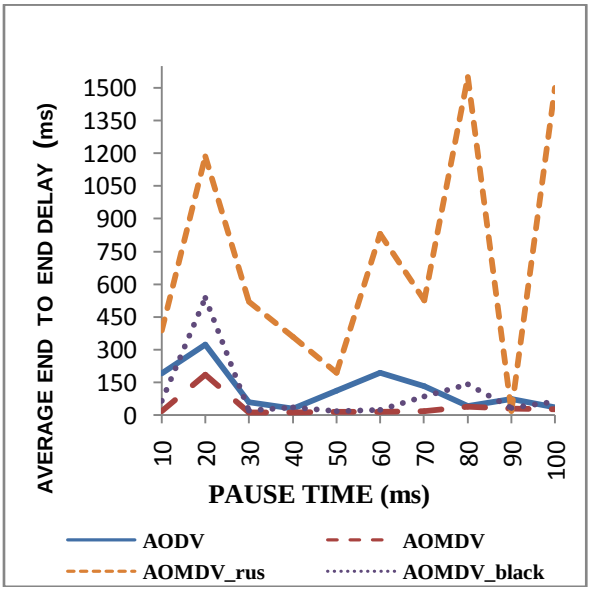

Figure 5.4: Average End To End Delay Vs. Pause Time

This shows that black hole attack will not affect the finding of multipath in AOMDV. So when any node exhibits black hole attacker characteristics during packet transmission, it can take the readily available alternate path for transmission, whereas this is not the case in the rushing attack.

Table 5.5: Average End To End Delay Vs. Pause Time

PAUSE TIME (ms)	Average End To End Delay (ms)			
	AODV	AODMV	AOMDV_rus	AOMDV_black
10	191.66	17.05	389.32	64.39
20	322.57	185.33	1187.14	537.24
30	57.819	12.33	518.84	20.78
40	28.98	10.94	359.47	36.811
50	112.36	16.13	194.62	19.04
60	192.65	16.01	830.15	24.57
70	133.17	19.08	527.26	85.25

80	40.65	38.11	1550	141.94
90	74.57	29.26	519	32.23
100	36.24	27.07	1500	60.81

The overall simulation study shows the impact of Rushing attack in AOMDV is more significant when compared to all other routing attacks like black hole attack. It is because the impact of this attack starts from the route discovery phase itself whereas other attacks show their impact only during transmission time. Since the rushing node acquires the path during route discovery phase itself, it can exhibit the characteristics of other routing attacks easily during transmission time. Also the impact of other routing attacks doesn't show much variation in AOMDV since it has an alternate path for transmission, whereas in rushing attack the discovered disjoint routes are very less and so there will be frequent route drops. One such attack, namely black hole attack is analysed in AOMDV and compared with rushing attack. The results show that the rushing attack affects the overall performance of AOMDV very badly than any other routing attack.

Conclusion and Future Work

Many research works have been carried out in the past decades to reduce routing attacks in AODV and DSR and less attention were shown on AOMDV. The routing attacks other than rushing attack can be overcome by choosing an alternate path by using multipath protocols like AOMDV protocol. This is not the case in rushing attack because it hinders the number of node disjoint paths formed during the route discovery phase. This causes frequent route drop during transmission time. It is intensively analysed and found that the end to end delay increases in AOMDV due to frequent route drops.

In future, the possible solution to overcome the rushing attack in AOMDV must be deployed in route discovery phase itself. This would safeguard AOMDV to generate disjoint paths without the interference of attacker node.

References

[1] Saleh Ali K. Al-Omari, Putra Sumari," An overview of Mobile Ad Hoc Networks for the existing protocols and applications," International Journal on applications of graph theory in wireless ad hoc networks and sensor networks (Graph-Hoc), Vol.2, No.1, March 2010.

[2] Charles E. Perkins and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing, " IEEE Computer Science Engineering, 2006.

[3] Perkins CE, Royer EM., "Ad hoc on-demand distance vector routing, "in *Proceedings of IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, 1999.

[4] Perkins CE, Belding-Royer E, Das SR. "Ad hoc on-demand distance vector (AODV) routing, "http://www.ietf.org/rfc/rfc3561.txt, July 2003, RFC 3561.

[5] M. K. Marina and S. R. Das, "On-demand Multipath Distance Vector Routing in Ad Hoc Networks, "in Proceedings of IEEE International Conference on Network Protocols (ICNP), pages 14–23, 2001.

[6] Mahesh K. Marina1*, † and Samir R. Das, " Ad hoc on-demand multipath distance vector routing, "Wireless Communications and Mobile Computing , *Wirel. Commun. Mob. Comput.* , 2006, 6, 969–988

[7] Sushi Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks, "Journal of Computing, Volume 3, issue 1,2151-2159,2011.

[8] Latha Tamilselvan and Dr. Sankaranarayanan, "Solution to Prevent Rushing Attack in Wireless Mobile Ad hoc Networks, "IEEE, 1215-1223, 2006.

[9] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attack and Defense in Wireless Ad Hoc Network Routing Protocols, "WiSe., 2003.

[10] Sathyam Shrivastava, "Rushing Attack and its Prevention Techniques, International Journal of Applied or Innovation in Engineering of Management (IJAIEM)," Volume 2, Issue4, April 2003.

[11] K. Ganesh Reddy, Dr. P., Santhi Thilagam, Bommena Nageswara Rao, "Cross-Layer IDS for Rushing Attack in Wireless Mesh Networks, "*CCSEIT-12*, October 26- 28, 2012, Coimbatore [Tamil Nadu, India] Copyright © 2012 ACM.

[12] Gajendra Singh Chandel and Rajul Chowksi, "Effect of Rushing Attack in AODV and its Prevention Technique, "International Journal of Computer Applications, Volume 83, 10-15, 2013.

[13] K. Vanaja and R. Umarani, "An Analysis of Single Path AODV Vs Multipath AOMDV on Link Break Using Ns-2," International Journal of Electronics, vol. 1, 2013.

[14] Mr. Hitesh Gupta, Mr.Shivshakti Shrivastav, Ms. Sanjana Sharma, "Detecting the DOS Attacks in AOMDV Using AOMDV-IDS Routing, "2013, 5th International Conference on Computational Intelligence and Communication Networks.

[15] Jyoti Rani and Naresh kumar, "Improving AOMDV protocol for Black Hole Detection in Mobile Ad hoc Network, "2013, International Conference on Control, Computing, Communication and Materials (ICCCCM).