International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 9-18
http://dx.doi.org/10.14257/ijsia.2015.9.4.02

Proposed Method to Enhance the Performance of AOMDV under DDOS Attack

[1]Kulbir Kaur Waraich and [2]Er.Simar Preet Singh

[1]*Research Scholar CSE Department, DAV University Jalandhar Punjab*
[2]*Assistant Professor CSE Department, DAV University Jalandhar Punjab*
[1]*sbmk91@gmail.com*
[2]*er.simarpreetsingh@gmail.com*

Abstract

Performance of AOMDV routing protocol is more reliable and efficient than other routing protocols in ad hoc network. It provides multipath routing which means it follows multipath to send data packets from source to destination. It do not follow multipath simultaneously but when failure occurs in one path, then it immediately discovers new path and then delivers packets up to destination. When any DDOS attack occurs in a network, then it degrades the performance of AOMDV routing protocol. Under this attack AOMDV consumes more power and bandwidth which further degrades the performance and makes it unreliable. In this paper a new protocol is proposed named EAOMDV i.e. Enhanced Ad hoc on demand distance vector routing protocol. It is enhance version of AOMDV which overcomes the problems that occurs during attack in AOMDV. In this, DDOS flooding attack is introduced. Then performance of existing and proposed protocol is measured under various parameters i.e. throughput, packet delivery ratio, end to end delay and normalized routing load.

Keywords**:** *AOMDV, EAOMDV, DDOS Flooding Attack, NS2, Delay, Throughput, Packet Delivery Ratio, end to end delay and Normalized Routing Load.*

1. Introduction

An Ad hoc Network consists of various mobile nodes that are interconnected with each other and forms a network without any centralized control and central administration. Ad hoc wireless networks perform the difficult task of multi-hop communication in an environment without a dedicated infrastructure, with mobile nodes and changing network topology [18] [4]. It is a dynamic wireless network that can be formed without the need for any pre-existing infrastructure in which each can act as a router [1]. Each and every device is free to move in any direction forming a network that is without any infrastructure and wires. Due to unique characteristics, such as dynamic network topology, limited bandwidth, and limited battery power, routing in a MANET is a particularly challenging task compared to a conventional network [2]. One of the key challenges in such networks is to design dynamic routing protocols are accomplishing scalability which makes it more efficient and reliable [10]. Selecting an appropriate routing protocol for steering data packets is a very important issue to evaluate the performance of MANETs [16]. Routing protocols can be on demand and table driven forming single and multipath. Among the on demand protocols, AOMDV is much better than single path routing protocols since it has a greater ability to reduce route discovery frequency as compared to single path routing protocols. In a single route discovery, AOMDV discovers multiple paths between source to destination.

In this paper a performance of AOMDV routing protocol with and without flooding attack is carried out and a new protocol is proposed i.e. EAOMDV (Enhanced AOMDV) which is enhance version of AOMDV. To cope with congestion and degradation of

ISSN: 1738-9976 IJSIA

communication quality, we proposed a solutions to improve the robustness of on-demand routing approach [13]. EAOMDV enhances the performance of AOMDV routing protocol and makes the whole network trust based in which nodes store only trust entries and makes entire network as a trust based network. Trust based network means it do not allow flooding attack to enter the network and has no effect on its performance. This scheme increases PDR and decreases delay thereby enhancing the trustworthiness in AOMDV based MANET routing [8].

2. Attacks in MANET

One of the serious attacks to be considered in MANET is DDoS attack. A DDoS attack is a large-scale, coordinated attack on the availability of services at a victim system or network resource [3]. Two types of DDos Attacks are active and passive attack [9]. The wireless nodes of MANET are thus susceptible to compromise and are particularly vulnerable to denial of service (DoS) attacks launched by malicious nodes or intruders [5]. The most common cases of attacks in mobile Ad hoc networks can be drop of routing packages and changes in the incoming packet which aims at disrupting the network routing and overall network reduce performance [14]. The main aim of DoS attack is the interruption of services by attempting to limit access to a machine or service instead of subverting the service itself [17].

3. Adhoc on Demand Multipath Distance Vector (AOMDV)

AOMDV is on demand and multipath distance vector which means it follows multiple routes or paths for sending data from source to destination. It is enhanced version of AODV that overcomes the problems that occur during node to node communication. The performance of AOMDV routing protocol is much better than AODV routing protocol. AOMDV routing protocol establishes node disjoint paths that have the lowest delays based on the interaction of many factors from different layers [6] and does not follow multiple paths simultaneously but update the path time to time. In AOMDV, source node sends route requests to all neighboring nodes with strong signal strength and the neighboring nodes forwards this request to other nodes. It is a distributed protocol that finds multiple link disjoint paths. When the first neighbor receives the packet it add a new field named first hop which creates the first hop list to keep a trace of the neighbors that generates a route request.

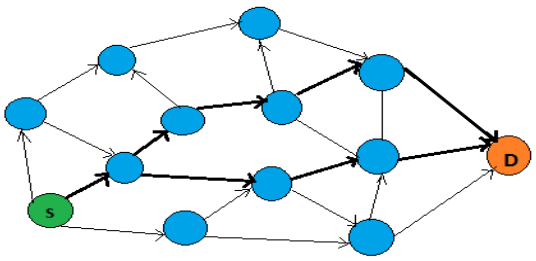

Figure 1. AOMDV Routing Protocol

4. Flooding Attack

Flooding attack is a denial of service attack which exhausts the network resources such as bandwidth consumption, power which affects the performance of routing protocol. Among various types of attacks, Flooding attack is more vulnerable to MANET [7]. Flooding Attack leads to data and route request flooding. It degrades the performance of routing protocol by generating large number of route requests as a result more bandwidth and power is consumed. This attack floods the network with so many fake route requests

so that the server slows down and legitimate nodes fails to send genuine requests. The network takes more time to synchronize.

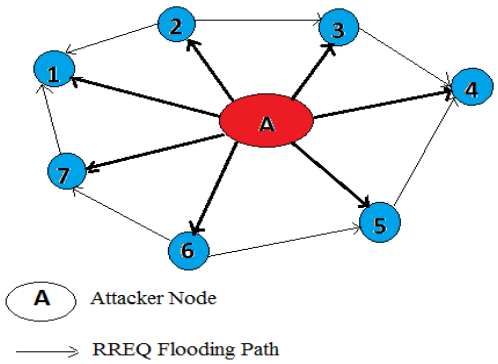

Figure 2. Flooding Attack

5. Enhance Ad hoc on Demand Multipath Routing Protocol (EAOMDV)

EAOMDV is enhanced version of AOMDV routing protocol. EAOMDV is trust based routing protocol. It consists of routing table which contains trust entries and make whole network as a trust based network. In this each node has its trust entry which contains trusted source_id and destination_id. It accepts only that nodes which have trusted values and it isolates nodes which have false values. EAOMDV establishes an efficient communication path between the source and destination nodes with minimum routing overhead [12]. The data packets send from source to destination from these trusted nodes. It do not allow attack to effect the network. This protocol determines the power required to preserve connectivity through nodes, in order to decrease interference and power consumption as well as to improve the network throughput [15].

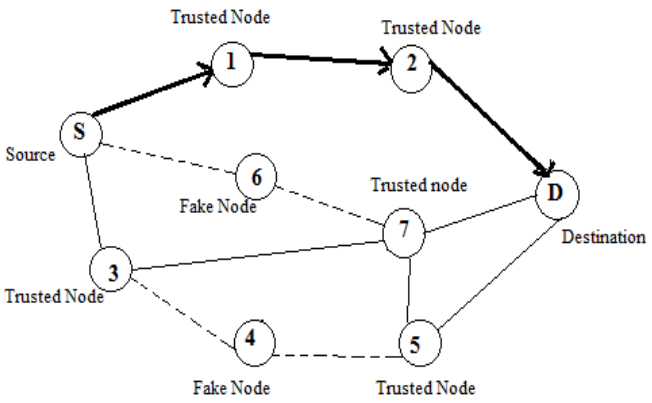

Figure 3. EAOMDV Routing Protocol

6. Simulation Methodology

Performance of AOMDV and EAOMDV is different according to their working. Simulation method is used to analyze the performance of these routing protocols before applying in real applications. In this work the performance of AOMDV and EAOMDV routing protocol is done by using NS2 (Network Simulator) tool.

6.1 NS2

NS2 is a network simulator data driven tool. NS2 provides users with executable command ns which take an input argument, the name of a tcl scripting file. Tcl simulation script is used by users as an input argument. Then simulation trace file is used to plot graphs or to create animation. NS2 contains two main languages i.e. C++ and OTcl (object oriented tool command language). The internal mechanisms of simulation objects are defined by C++ language. Assembling and configuration of objects as well as scheduling discrete events are set up by OTcl language. NS2 runs on various platforms like UNIX, Windows and Mac systems [19].

6.2 AWK Script

AWK Script is used to extract the data from trace files that are generated by simulator tool during simulation [20]. AWK script is used to search files according to certain patterns. These certain patterns contain lines. A specified action is used when a line matches a pattern. It keeps processing and matching these lines until it reaches to end. Then data extraction takes place from these lines. The awk script is run according to following command:
awk –f programfile tracefile

The format of AWK script:
BEGIN {print “START”}
{ print }
END {print “STOP”}
Begin part comprises of initialization of variable.
End part having the formulation according to which data is extract from trace file.

7. Performance Metrics

The aim of our work is to examine and analyze the effect of various factors and parameters on performance of AOMDV routing protocol with and without flooding attack and EAOMDV routing protocol. The performance is different in different parameters. In this work parameters used are Throughput, packet delivery ratio, end to end delay and normalized routing load. The tcl coding is used to define all the parameters and all models which are used in performance analysis. The ns simulator is creating which means it makes a scenario file which run in network simulator. The Random Waypoint Mobility model is used according to which the node moves. The IEEE 802.11 Mac model is used. Trace file is created which trace all the data which is written in tcl. Position and movement of nodes is defined so that it finds a route from source to destination to send the data packets from source to destination. The CBR and UDP traffic is used which has different effect on the performance of the protocol. The simulation time of whole simulations is 120 s after 120 sec the simulation stops. Mac 802.11 used as a physical layer, UDP as Transport layer and CBR as application layer. The parameters in our simulation are reported in table 1.

7.1 Parameters

7.1.1 Throughput: 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.*

7.1.2 Packet Delivery Ratio: The ratio of packets that are successfully delivered to the number of packets that have been sent. Formula to calculate Packet Delivery Ratio is:

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

7.1.3 End to End Delay: Time taken by data packet to transfer from source to destination across the network. Formula to calculate End to end Delay is:

End to End Delay = Transmission Delay+Propagation Time+Procvessing Delay+Queuing Delay

7.1.4 Normalized Routing Load: The number of routing packets transmitted per data packet delivered at the destination. This metric gives an idea of the extra bandwidth consumed by overhead to deliver data packet.

*NRL= ((Control Packet Sent + Control Packet Forward) /Data Packet Received)*100*

8. Result Analysis

In this work, performance of AOMDV routing protocol with and without flooding attack is carried out under various parameters. Also a new protocol is proposed named EAOMDV (Enhance Ad hoc on demand multipath distance vector) and its performance is analyzed under given parameters.

Table 1. Simulation Parameters

SIMULATION PARAMETERS	VALUE
Channel	Wireless
Propagation Model	Two Ray Ground
Mac Address	802.11
Packet Size	512 bytes
Duration	120 sec
Routing Protocols	AOMDV and EAOMDV
Attack	DDOS Flooding Attack
Connection Type	UDP, CBR
Simulation Area (sq. m)	1000x1000
Number of nodes	20, 40, 60,80,100

8.1 Graphs

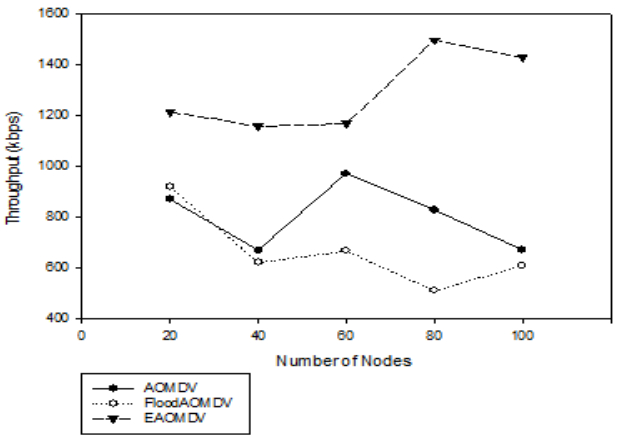

Figure 4. Throughput (kbps)

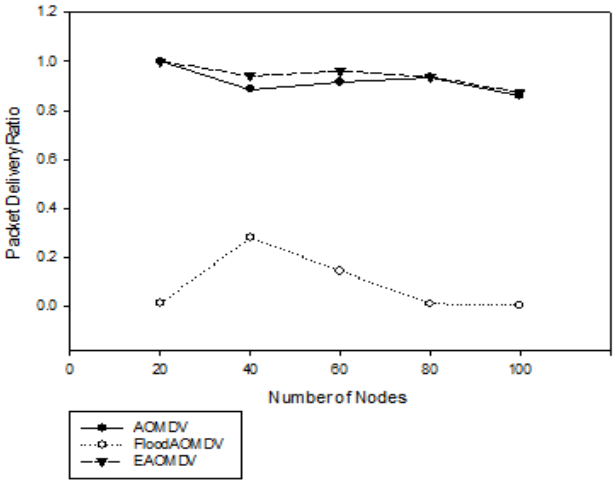

Figure 5. Packet Delivery Ratio

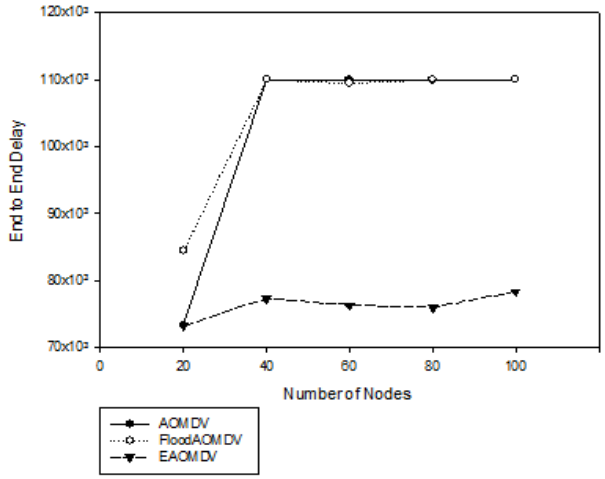

Figure 6. End to end Delay

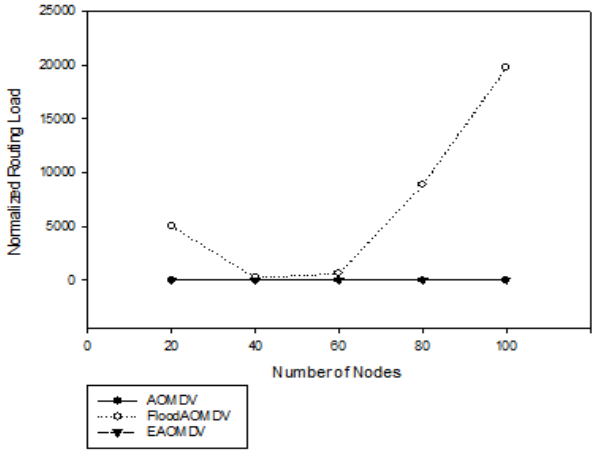

Figure 7. Normalized Routing Delay

In this section, the graph shows variation of routing protocols with different parameters. In Figure 4, the variation of throughput is shown in which throughput of EAOMDV routing protocol is more than AOMDV protocol and flooding AOMDV. As the number of nodes increases the throughput also increases. In Figure 5, the variation of packet delivery ratio is shown. The number of packets delivered in EAOMDV is more than AOMDV and Flood AOMDV which means EAOMDV delivers more packets from source to destination. Figure 6 shows the end to end delay that occurs from source to destination. In AOMDV and Flood AOMDV the delay is almost same but slightly more in flood AOMDV. Figure 7 shows normalized routing delay in which flood AOMDV requires more routing load to be normalized because of flooding attack in the network. AOMDV and EAOMDV requires less routing load to be normalized.

9. Conclusion

In this paper, the performance of AOMDV routing protocol is carried out with and without Flooding attack and new protocol is proposed named EAOMDV and its performance is analyzed. Different measuring parameters are used i.e. Throughput, packet delivery ratio, end to end delay and normalized routing load. Performance of AOMDV degrades when Ddos flooding attack occurs in the network.

Table 2. Performance Analysis of AOMDV, Flood AOMDV and EAOMDV

	No of Nodes	Through put	PDR	Delay	NRL
AOMDV	20	870.60	1.0000	73366.8	0.955
	40	669.20	0.8866	109971	2.257
	60	971.43	0.9141	109969	3.186
	80	828.59	0.9360	109942	4.120
	100	671.78	0.8578	109953	5.810
	No of Nodes	Through put	PDR	Delay	NRL
Flood AOMDV	20	918.92	0.0133	84453.5	4986.290
	40	621.74	0.2814	109966	214.169
	60	667.28	0.1452	109434	601.087
	80	510.07	0.0117	109956	8865.889
	100	610.02	0.0057	109954	19760.231
	No of Nodes	Through put	PDR	Delay	NRL
EAOMDV	20	1215.21	1.0000	73305.5	0.951
	40	1158.44	0.9410	77355.3	2.079
	60	1168.49	0.9604	76321.4	3.046
	80	1496.14	0.9359	76035.3	4.110
	100	1429.83	0.8737	78328.7	5.661

EAOMDV performs better than AOMDV routing protocol which do not allow flooding attack to enter the network. EAOMDV makes the whole network as a trust based network and its performance is better in all parameters. In Future work can be done on different ddos attacks and performance of AOMDV and EAOMDV will be analyzed. Also, various detection and prevention techniques can be applied to avoid these attacks.

References

[1] H. D. Trung, W. Benjapolakul and P. M. Duc, "Performance evaluation and comparison of different ad hoc routing protocols", Elsevier, Computer communications, Security on Wireless ad hoc and sensor networks, vol. 30, **(2007)**.
[2] B. Kannhavong, H. Nakayama, Yoshiakinemoto and N. Kato, "A Survey of Routing attacks in Mobile Ad Hoc Networks", IEEE, Security in Wireless Mobile Ad hoc and Sensor Networks, **(2007)**.
[3] S. A. Arunmozhi and Y. Venkataramani, "A New Defense Scheme against DDoS Attack in Mobile Ad Hoc Networks", Springer, Advance computing Communications in Computer and Information Science, vol. 133, **(2011)**.
[4 A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Boloni and D. Turgut, "Routing Protocols in ad hoc networks: A survey", Elsevier, Computer Networks, vol. 55, no. 13, **(2011)**.
[5] A. Bandyopadhyay, S. Vuppala and P.Choudhury, "A Simulation analysis of flooding attack in MANET using NS-3, IEEE", 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Electronic Systems Technology (Wireless VITAE), **(2011)**.
[6] M. Obaidat, M.A Ali and S. Obeidat, "A Novel Multipath Routing Protocol for MANETs", IEEE 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), **(2011)**.
[7] P. Choudhury, S. Nandi, A. Pal and N. C. Debnath, "Mitigating rout request flooding attack in MANET using node reputation", IEEE, International Conference on Industrial Informatics (INDIN), **(2012)**.
[8] S. Subramanian and B. Ramachandran, "Trusted AODV for Trustworthy Routing in MANET", Springer, Advances in Computer Sciences, engineering and Applications, vol. 167, **(2012)**.
[9] M. Chhabra, B. Gupta and A. Almomani, "A Novel Solution to Handle DDOS Attack in MANET", Scientific Research, Journal of Information Security, **(2013)**.
[10] B. Rekha and D. V. Ashoka, "Performance Analysis of AODV and AOMDV Routing Protocols on scalability for MANETs", Springer, Emerging Research in Electronics, Computer Science and Technology, **(2013)**.
[11] P. A. Lotfy and M. A. Azer, "Performance evaluation of AODV under dos attacks", IEEE, 6th Joint IFIP on Wireless and Mobile Networking Conference (WMNC), **(2013)**.
[12] T. A. Alahdal and S. Mohammad, "Performance of standardized routing protocols in ad-hoc networks", IEEE International Conference on Computing, Electrical and Electronics Engineering (ICCEEE), **(2013)**.
[13] T. Yelemou, "New approach to improve the robustness of AOMDV protocol", IEEE 10th International Multi-Conference on Systems, Signals and Devices (SSD), **(2013)**.
[14] H. Gupta, S. Shrivastav and S. Sharma, "Detecting the DOS Attacks in AOMDV Using AOMDV-IDS Routing", IEEE 5th International Conference on Computational Intelligence and communication Networks (CICN), **(2013)**.
[15] A. M. Bamhdi, P. King and P. J. B., "Performance evaluation of Dynamic-Power AODV, AOMDV, AODV and DSR protocols in MANETs", IEEE International Conference on Smart communications in Network Technologies (SaCoNet), **(2013)**.
[16] T. K. Araghi, M. Zamani and A. B. T. A. Mnaf, "Performance Analysis in Reactive Routing Protocols in Wireless Mobile Ad Hoc Networks Using DSR", AODV and AOMDV, IEEE, International Conference on Informatics and Creative Multimedia (ICICM), **(2013)**.
[17] K. K. Waraich and R. Kaur, "Security against DDoS Attack in MANETs", International Journal of computer Science and Mobile Computing, vol. 3, **(2014)**.
[18] S. P. Singh and B. Singh, "Routing Algorithm in MANET", International Journal of Engineering and Innovative Technology, vol. 3, **(2014)**.
[19] T. Issariyakul and E. Hossain, "Introduction to Network Simulator NS2", Springer Science and Business Media, LLC, **(2009)**.
[20] A. D. Robins, GAWK:an effective AWK programming, 3rd ed, **(2010)**.

Authors

Kulbir Kaur Waraich, she is a Research Scholar Computer Science & Engineering Department from DAV University Jalandhar, Punjab (INDIA). B.Tech. Professional with specialization in Information Technology from SBBSIET (PTU) Jalandhar, Punjab (INDIA). Member of Computer Society of India. Participated in Paper Presentation organized during National Conference on impact of Science and tech. Research Publications in various international journals.

Er. Simar Preet Singh, he received the degree of B.Tech (Computer Science & Engineering) from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib (India) in 2009 and M.Tech (Computer Science & Engineering) from Punjabi University, Patiala (India), in 2011. He has worked in Infosys Limited for two years. He is a lifetime member of HANS Anti-Hacking Anticipation Society, India. Apart from this, he is also having certifications like Microsoft Certified Systems Engineer (MCSE), Microsoft Certified Technology Specialist (MCTS) and Core Java. He had undergone training programmer for VB.Net and Cisco Certified Network Associates (CCNA). He has presented many research papers in various National and International Journals/Conferences in India and abroad. His area of interest includes Database, Network Security and Network Management. He is presently working as Assistant Professor in Computer Science & Engineering at DAV University, Jalandhar (India).