International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

Study and Evaluation of DSR and AODV MANET Routing Protocols under Flooding and Rushing Attacks

Monika Verma
M.E. Scholar, Department of Computer Science & Engg.
M.B.M. Engineering College, J.N.V. University
Jodhpur, India

Dr. N. C. Barwar
Assoc. Prof., Department of Computer Science & Engg.
M.B.M. Engineering College, J.N.V. University
Jodhpur, India

***Abstract*— Over the past decade, there has been a lot of research in the area of Mobile Ad-hoc NETwork(MANET). A MANET is infrastructure-less network where nodes communicate with each other without any centralized administration. Due to its nature routing security is challenging task and it is vulnerable to various types of attacks. The Flooding and Rushing attacks are well known attacks of MANET. In this paper the performance of MANET routing protocols, AODV and DSR, with flooding and rushing attack have been analyzed under different scenarios using CBR traffic using NS2 taking various parameters such packet delivery ratio, average end to end delay and average throughput to compare and evaluate their performance.**

Keywords—MANET, AODV, DSR, Flooding, Rushing

I. INTRODUCTION

In mobile ad-hoc network (MANET) nodes communicate without use of pre-defined infrastructure, so it is called infrastructure-less network [1]. Nodes are free to move randomly and their topology changed dynamically. Therefore MANET has unique characteristics such as lack of centralized administration, distributed cooperation, limited bandwidth, and limited battery power [2]. These characteristics make routing in a MANET a challenging task. There are many routing protocols available for MANET which is broadly classified into three types: proactive (or table-driven), reactive (or on-demand) and hybrid. Generally, MANET often suffers from security attacks because of its features, many of them targets the routing protocols [6] [13]. The attacks on routing protocols can generally be classified as passive and active attacks [12] [14]. Flooding and Rushing attacks are kind of active attack.

II. MANET ROUTING PROTOCOLS

A. Dynamic Source Routing (DSR)

DSR is a reactive MANET routing protocol means it discovers a route to destination only when it is required. It uses source routing in which source is responsible for providing information of whole path [3] [9]. There is no need of any beacon in DSR. Basically DSR maintains two phases: Route Discovery and Route Maintenance as shown in Fig. 1 and 2. In Route Discovery phase source finds path to destination by broadcasting RREQ packet. Each node retransmits the RREQ packet if it has not forwarded a copy of it, provided that the Time-To-Live has not been exceeded. Each RREQ carries a sequence number generated by the source node and the path it has traversed. In this protocol intermediate node uses cache that stores all possible information extracted from the source route contained in a data packet. When destination receives the RREQ packet, it sends a RREP packet to source node, listing the route taken by request packet. Source node selects route with lowest latency. In route maintenance, whenever a link break, the RERR packet propagates to the original source, which in turn initiates a new route discovery process. DSR also allows piggy-backing.

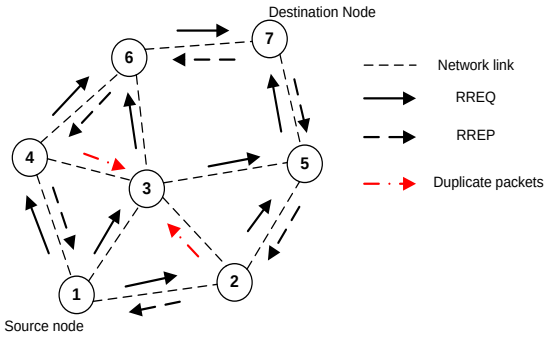

Fig. 1 Route Discovery in DSR

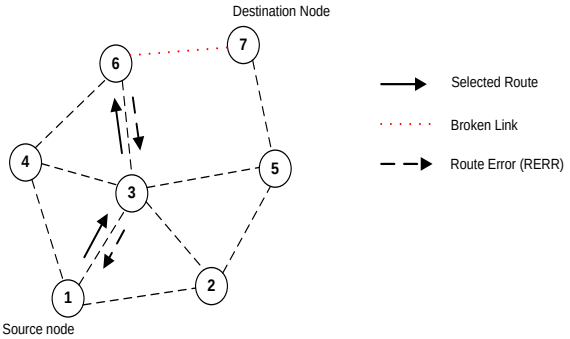

Fig.2 Route Maintenance in DSR

B. *Ad-Hoc On-Demand Distance Vector(AODV)*

Ad hoc On-Demand Distance Vector (AODV) is also an on-demand MANET routing protocol [4] [7]. Basically AODV maintains two phases: Route Discovery and Route Maintenance as shown in Fig. 3 and 4. AODV finds routes using the route discovery process similar to DSR and uses destination sequence numbers to compute fresh routes. In route discovery phase, source node broadcast RREQ packet like DSR. This packet contains the source identifier (SId), the destination identifier (DId), the source sequence number (SSeq), the destination sequence numbers (DSeq), the broadcast identifier (BId) and TTL fields. When an intermediate node receives a RREQ packet, it either forwards it or sends RREP packet to source, if it has a valid route to the destination in its cache. The pair of SId and BId is used to detect if the node has received an earlier copy of the RREQ. Before forwarding RREQ, every intermediate node store the previous node's address and it's BId. Intermediate node also maintains a timer with every entry to delete RREQ if reply is not received before it expires. Whenever a RREP is received by a node, it stores the information of the previous node, thus each node maintains only the next hop information. In route maintenance, whenever a link break, the RERR packet propagates to the source, which again initiates a new route discovery process.

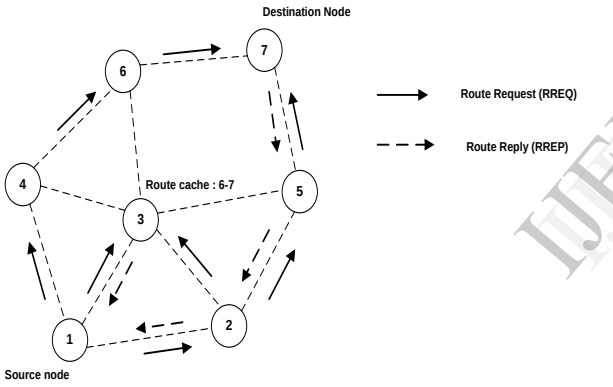

Fig. 3 Route discovery in AODV

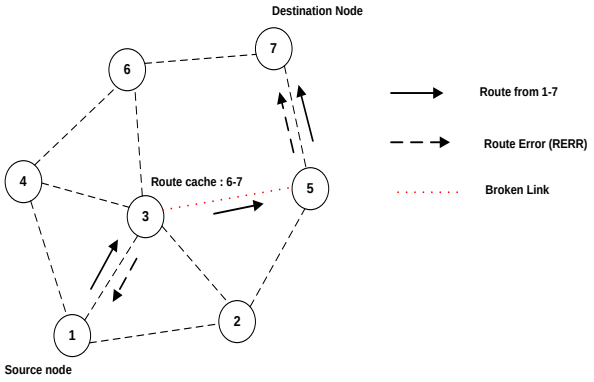

Fig. 4 Route Maintenance in AODV

III. MANET ROUTING ATTACKS

A. *Flooding Aattack*

In RREQ flooding attack, Attacker generates more number of RREQ packets to a node which does not exist in network [5] [10]. The priority of RREQ is higher than data packets so handled first so this becomes a honey pot for attacker. The purpose of this attack is to consume bandwidth and to exhaust network resources all time [11] [12].

B. *Rushing Attack*

Rushing is a zero delay attack [5]. It is more dangerous when attacker nearby source or destination. Reactive routing protocols are more vulnerable to this attack because whenever source node broadcast RREQ packets, a malicious node receives that and forward without any hop_count update and delay in to the network. When legitimate nodes receive original RREQ packets, they are dropped because it already received packet from adversary and treat this as a duplicate packets. Thus, attacker included in active route and disrupts data forwarding. Rushing attacker disturbs the data forwarding phase by either jellyfish or byzantine attack.

IV. NS2 SIMULATION

Network Simulator is event driven object oriented simulator [8]. It uses OTcl (Object oriented Tool Command Language) programming language to interpret user simulation scripts and Tcl language is fully compatible with the C++. NS is an interpreter of Tcl scripts of the users; they work together with C++ codes.

A. *Performance Metrics*

The following performance metrics are considered for evaluation of MANET routing protocols:

1) Packet Delivery Ratio: The ratio of the data packets delivered to the destination to those generated by the source.

2) Average End to End Delay: This metrics represents average end-to-end delay that indicates how long it took for a packet to travel from the source to the application layer of the destination.

3) Average Throughput: This metrics represents the average number of bits arrived per second at destination and measured in bps.

In this work NS simulator is used for the simulation. Mobility scenarios that are generated by using a random way point model by varying 25 to 150 nodes moving in simulation area of 1000m x 1000m. Table I show the parameters used in simulation.

TABLE I. SIMULATION PARAMETERS

Simulator	NS-2 (version 2.35)
Simulation Time	500 (s)
Number of Nodes	25,50,75,100,125,150
Simulation Area	1000 x 1000m
Routing Protocols	AODV and DSR
Traffic	CBR(Constant Bit Rate)
Pause Time	10 (ms)
Packet Size	512 bytes
Movement Model	Random Way Point

B. Simulation Results and Performance Analysis

Fig. 5 shows that packet delivery ratio of AODV is less affected than DSR because it maintains a timer at every intermediate node in the network.

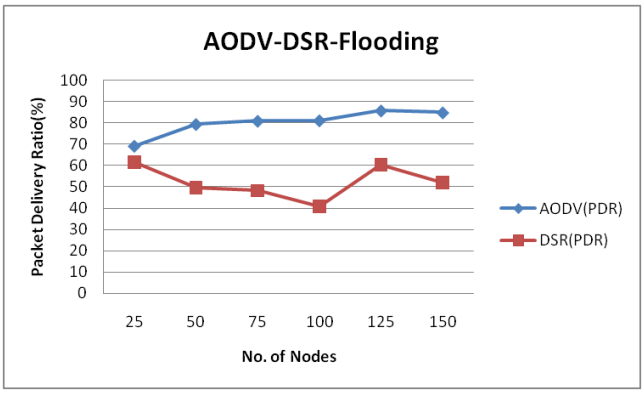

Fig. 5: Packet Delivery Ratio of AODV and DSR with flooding attack

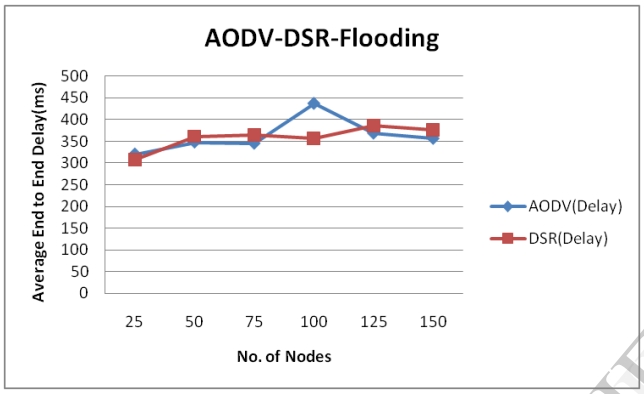

Fig. 6: Average End to End Delay of AODV and DSR with flooding attack

Fig. 6 shows that average end to end delay of DSR is slightly greater than AODV due to route cache overhead of DSR.

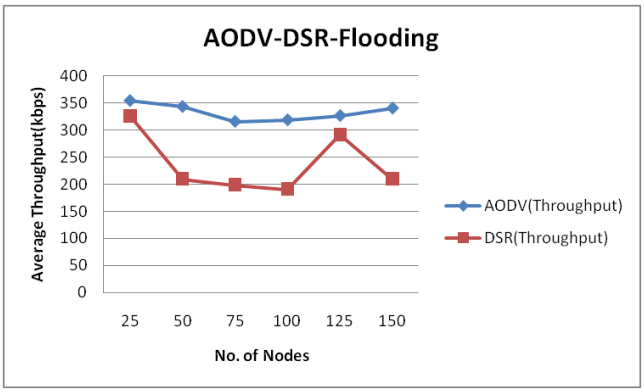

Fig. 7: Average Throughput of AODV and DSR with flooding attack

Fig. 7 shows that average throughput of AODV is higher than DSR because presence of timer in AODV which slightly reduce the effect of flooder.

From the overall observation of AODV and DSR routing protocols under route request flooding attack it observed that AODV outperforms compare to DSR because AODV inherits the good feature of DSDV and DSR.

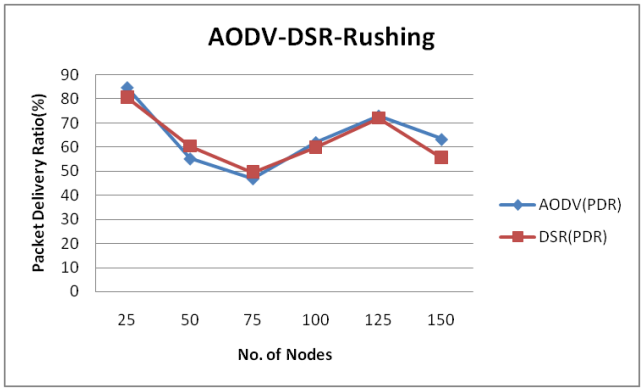

Fig. 8: Packet Delivery Ratio of AODV and DSR with rushing attack

Fig. 8 shows the packet delivery ratio of AODV and DSR routing protocols under rushing attack. This graph shows that packet delivery ratio in DSR and AODV adopting similar patterns as increasing the number of nodes due to on-demand nature of these protocols.

Fig. 9 shows the end to end delay of AODV and DSR under the rushing attack with increasing number of nodes. Delay of both routing protocols is increase in the presence of rushing attack but delay of DSR in slightly higher than AODV due to cache overhead.

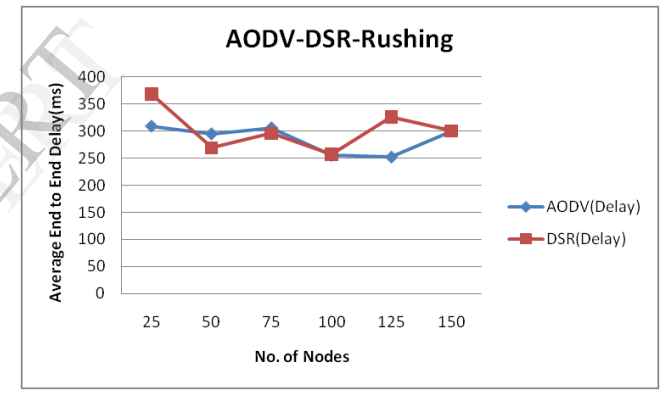

Fig. 9: Average End to End Delay of AODV and DSR with rushing attack

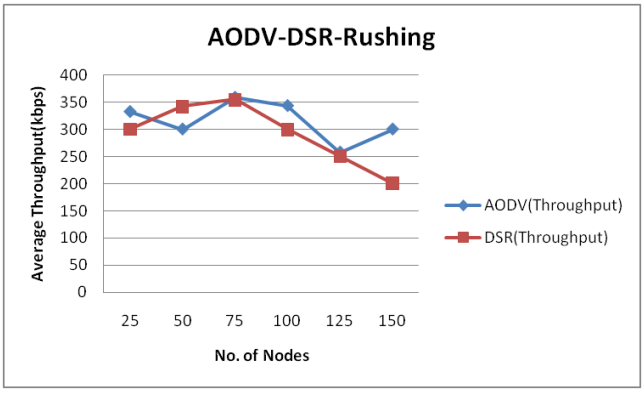

Fig. 10: Average Throughput of AODV and DSR with rushing attack

Fig. 10 shows the AODV and DSR routing protocols in effect of rushing attack. Average throughput of both routing protocols is decrease in the presence of rushing attack but DSR has less throughput than AODV.

From the overall observation of AODV and DSR routing protocols under rushing attack which also following jelly fish and byzantine attack, it observed that AODV performs better than DSR because AODV working hop-by-hop routing.

V. CONCLUSION

In this paper, performance analysis of flooding and rushing attacks under CBR traffic in different scenarios taking AODV and DSR MANET routing protocols are simulated under NS2. Different performance metrics like Packet Delivery Ratio, Average End to End Delay and Average Throughput are considered for analysis. It is inferred that (i) Packet delivery ratio of DSR is less than AODV in flooding as well as rushing attack but from the overall analysis it is also observed that in given scenarios AODV is more affected by flooding attack when number of nodes are less but when number of nodes increased then AODV is more affected by rushing attack as compared to flooding attack and effect of flooding attack on DSR is more as compare to rushing attack. (ii) Average end to end delay is higher in DSR as compare to AODV in flooding and rushing attack but the overall delay of both the protocols improves in rushing attack as compared to flooding attack. (iii) Average throughput of DSR is less than AODV in flooding and rushing attack but in the given scenarios it is observed that in high node density throughput of both routing protocols is more affected by rushing attack as compare to flooding attack.

REFERENCES

[1] S. Basagni, M.Conti, S. Giordano and I. Stojmenovic, "Mobile Ad Hoc Networking", A John Wiley & Sons, Inc., Publication, 2004, ISBN 0-471-37313-3.
[2] Imrich Chlamtac, Marco Conti and Jennifer J.-N.Liu, "Mobile ad hoc networking: imperatives and challenges", Ad Hoc Networks 2003 Elsevier.
[3] D B. Johnson, D A. Maltz, and Y. Hu, "The Dynamic Source Routing Protocol For Mobile Ad Hoc Network", Internet-Draft, July 2004.
[4] C.E. Perkins, E. Royer, and S.R. Das, "Ad Hoc On Demand DistanceVector(AODV) Routing," Internet Draft, July 2003.
[5] Amara korba, Abdelaziz, Mehdi Nafaa and Ghanemi Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", 15th International Conference on Computer Modelling and Simulation, 2013 IEEE.
[6] H.Deng, W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks", University of Cincinnati, IEEE Communication Magzine, Oct, 2002.
[7] Mohammed Saeed Alkatheiri, Jianwei Liu and Abdur Rashid Sangi, "AODV Routing Protocol Under Several Routing Attacks in MANETs", 978-1-61284-307-0/11, 2011 IEEE.
[8] [Online]. Available: http://www.isi.edu/nsnam/ns
[9] Bryan Hogan (2010) [Online]. Available: http://www.skynet.ie/~bryan/dsr_faq/
[10] Meenakshi Patel, Sanjay Sharma and Divya Sharan, "Detection and Prevention of Flooding Attack Using SVM", International Conference on Communication Systems and Network Technologies, 978-0-7695-4958-3/13, 2013 IEEE.
[11] Ping Yi, Zhoulin Dai, Yiping Zhong and Shiyong Zhang, "Resisting Flooding Attacks in Ad Hoc Networks", Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05),IEEE.
[12] Neeraj Arora and Dr. N.C. Barwar, "Performance Analysis of Black Hole Attack on different MANET Routing Protocols", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014.
[13] Namrata Marium Chacko, Shini sam and P.Getzi Jeba Leelipushpam, "A survey on various privacy and security features adopted in MANETs routing Protocol", 978-1-4673-5090-7/2013 IEEE.
[14] Neeraj Arora and Dr. N. C. Barwar, "Performance Analysis of DSDV, AODV and ZRP under Blackhole attack", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 4, April – 2014.