Analysing Performance Disruption of MANET Under Explicit Flooding Attack Frequency

Priyanka Wadhwani and Sourabh Singh Verma

Abstract The number of routing protocol is available in Mobile Ad hoc Networks (MANETs), but none of them is perfect as it is hard to achieve the security in it. The MANETs is in vulnerable of different attacks because the network is scalable and has very dynamic mobile nodes. The performance of protocols is severely affected in the presence of malicious nodes as these causes routing information to be erroneous and introduces excessive traffic load and inefficient routing. In this paper, we analyse the network performance extensively using Ad hoc On Demand Distance Vector (AODV) routing protocol in the presence of a flooding attack with specific frequency rate. The NS2 network simulator is used to analyse this flooding attack on AODV and its impact are shown using various performance metrics like Packet Delivery Ratio (PDR), throughput with variable flooding rates and malicious nodes etc.

Keywords Flooding · Attack · Flood frequency · AODV · RREQ flooding · MANET

1 Introduction

Mobile ad hoc networks (MANETs) are significantly different and more complex from the wired networks as it is composed of autonomous wireless nodes. These nodes are mobile thus topology of the network gets changed over the period of time and due to this node are susceptible to malicious attacks [1]. There are a large number of known attacks against MANET like flooding, black hole, wormhole, sinkhole, etc. These attacks cause hazards on the network by manipulating the

P. Wadhwani (✉) · S.S. Verma
Mody University of Science and Technology, CET, Lakshmangarh, Rajasthan, India
e-mail: wadhwanipriyanka@ymail.com

S.S. Verma
e-mail: ssverma.cet@modyuniversity.ac.in

S.C. Satapathy and S. Das (eds.), *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 2*, Smart Innovation, Systems and Technologies 51, DOI 10.1007/978-3-319-30927-9_6

parameters of routing messages and traversing the packet in the wrong direction. Among these attacks, we have evaluated RREQ flooding attack. During a flooding attack [2], attacker floods the entire network by sending a number of fake messages to unknown destination nodes. Such an attack can be categorized as RREQ flooding, data packet flooding and Hello message flooding, explained as follows.

RREQ flooding: During the route discovery process of the routing protocol, malicious node floods fake RREQ message and broadcast them through intermediate nodes in the network till the destination is reached which is non-existent. Unnecessarily forwarding these fake RREQ packets results in network congestion and an overflow of route table. Due to which intermediate nodes in the network are busy to transmit such control packets and data packets remains unsent or may be dropped. This degrades throughput and increases consumption of energy [3].

Data Flooding: Route discovery process towards the destination node of routing protocol is maintained by the attacker (malicious nodes) and then frequently sends a large number of useless data packets along the path. On receiving excessive packets from the attacker, will result in wastage of bandwidth and thus nodes were unable to communicate efficiently.

Hello Flood: Nodes broadcast hello packets at specific interval to know all its neighbouring. On receiving a Hello message from a neighbour node, route tables are updated so that it may also not contain any stale entry. Flooding of hello message with high frequency makes nearby nodes unable to process the data. This result increases routing overhead.

The rest of the paper is organized as follows: Sect. 2 gives a literature survey, Sect. 3 contains the simulation parameters used followed by the simulation results and Sect. 4 concluding remarks.

2 Literature Survey

Number of researches [4, 5] has been made in finding out malicious node attacks. In a MANET, different types of devices exist and work together in a cooperative manner while it is quite unfair to restrict all these devices with some threshold value.

Reference [3] discussed implementation and analysis of different attacks in AODV and how these attacks effect packet efficiency and throughput of the network. Study of routing attacks in MANETs by making AODV work maliciously, call it malicious AODV. Routing in ad hoc networks [6] has been a challenge since wireless network came into existence and hence dynamic routing protocols are needed to function properly (e.g. AODV, DSR). As AODV [7], on demand routing protocol discovers a route to a destination only when required. A malicious node abuses route discovery mechanism of AODV to result in Denial of Service attack and these nodes prevent other nodes from establishing a path by sending fake routing information.

Due to network load imposed by fake RREQ and useless data packets [8], a non-malicious node cannot serve other nodes and leads to wastage of bandwidth, overflow

of routing table entries and wastage of nodes' processing time. A malicious node may be responsible for these attacks; due to flooding [9] the network with large number of route request to invalid destination creates dramatic impact over the performance of the protocol. Such as AODV performs worse when packet loss increases with increase in the number of fake RREQ packets and as the mobility decreases i.e., the pause time increases the packet efficiency improves, but not substantially.

References [10, 11] discussed how flooding affects the performance, particularly with variable duration of flooding nodes considering a different number of malicious nodes. It is observed if flood node is active for more time than it shows drastic effect on Quality of service (QOS) parameters of the network. Further, it was shown that how throughput and bandwidth consumed by flood RREQ are inversely proportion to each other.

In [12] discussed how route disruption, resource consumption effect AODV protocol over performance metrics as the number of data packets sent and received. In [13] influence of flooding attack is analysed under the circumstances of different parameter on the entire network, including number of attack nodes, network bandwidth and number of normal nodes. Reference [14] provides a common set of security needs for routing protocols that are subject towards attack. These attacks can harm the network operations or the individual user as a whole. This paper discussed about the attacks against well-considered, well-defined implementation of routing protocols. Reference [15] provides a comparison of all routing protocols' performance and determines which protocol performs best under different number of network scenarios. Traditional TCP/IP structure is being employed by MANETs and each layer in TCP/IP model requires modification to function efficiently in it.

In our paper, we took an approach which shows flooding effect with variable mobile node speed, constant bit rate (CBR) in packets per second and connections between nodes considering over different flood frequency and malicious nodes.

3 Simulation Results

In order to simulate the impact of flooding attack in MANET performance, the AODV routing protocol was modified to add malicious nodes. In our evaluation, we are tracing performance metrics with varying speed of nodes, connections between nodes and CBR rates over a different number of flooding nodes and variable flood rates.

3.1 Performance Metrics

PDR (Packet Delivery Ratio)—the number of delivered data packet to the total packets to be delivered by the node. The larger number of pdr means better performance of the nodes.

Throughput—total amount of data in terms of number of bytes received by the destination per second measured in kbps. For better performance of nodes in the network, throughput should be larger with less mobility of nodes.

3.2 Simulation Setup

All evaluation is done using NS2 [16]. Our simulation uses following setup: (Table 1).

We have run the simulations as shown in Table 1 various times by using all the parameters mentioned and log the traffic of our created network in number of conditions and results are processed for further evaluation.

3.3 Results and Discussion

PDR over number of flooding nodes (2, 4) with varying nodes' speed: Our result in Fig. 1 shows on increasing speed of nodes, greater % of PDR results for network with less malicious nodes and lesser % of PDR for network with more malicious nodes at constant flooding rate. Thus, due the impact of request flooding attack number of malicious node at greater speed increases packet loss and decreases efficiency of the routing protocol.

Throughput over number of flooding nodes (2, 4) with varying speed of nodes: Our result in Fig. 2 shows on increasing mobility speed throughput gets decreased for more number of malicious nodes as wastage of bandwidth gets more due impact of flooding attack in the network. As it is shown that at 10 m/s speed of nodes, throughput is 69 kbps for 2 malicious nodes and 13 kbps for 4 malicious nodes.

Table 1 Simulation parameters and their values

Simulation parameters	Value
Simulation time	50 s
No. of nodes	50
Area	500 × 500 m
Traffic	CBR (constant bit rate)
CBR rate	5, 10, 15, 20, 25, 30
Motion	Random
Routing protocol	AODV
No. of flooding nodes	2, 4
Flooding rates	0.05, 0.1
Transport layer	UDP
Node motion	Random
Node max speed	10, 20, 30, 40, 50 m/s

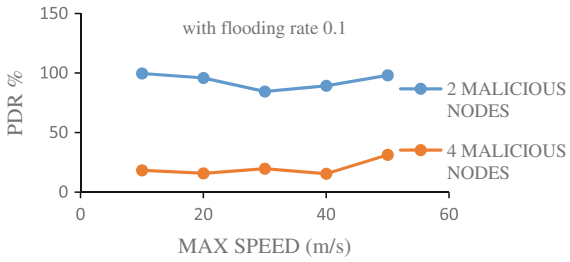

Fig. 1 PDR versus max speed

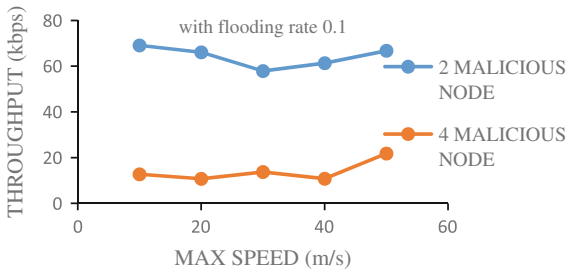

Fig. 2 Throughput versus max speed

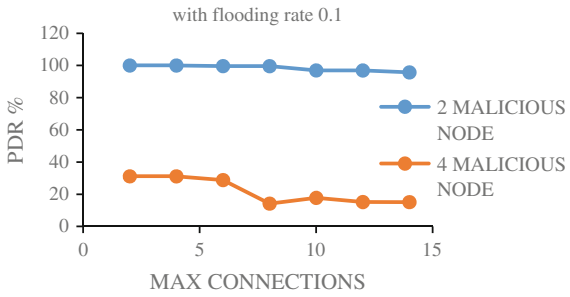

Fig. 3 PDR versus maximum connections

PDR over number of malicious node (2, 4) with varying connections between nodes: Our result in Fig. 3 shows on increasing connections between nodes PDR decreases with increase in malicious nodes at same flooding rate. As it is shown that PDR with 5 connections is 100 % for 2 malicious nodes and 30 % for 4 malicious nodes.

Throughput over number of malicious nodes (2, 4) with varying connections between nodes: In Fig. 4 result shows on increasing connections between nodes throughput decreases with increase in malicious node in the network. As shown that throughput with 5 connection is 35 kbps for 2 malicious node and 11 kbps for 4 malicious nodes at 0.1 flooding rate.

PDR over flooding rates (0.05, 0.1) with varying CBR rate: In Fig. 5 results shows that on increasing CBR rate, PDR increases with increase in flooding rate. But at constant flooding rate PDR decreases with increase in CBR due to impact of

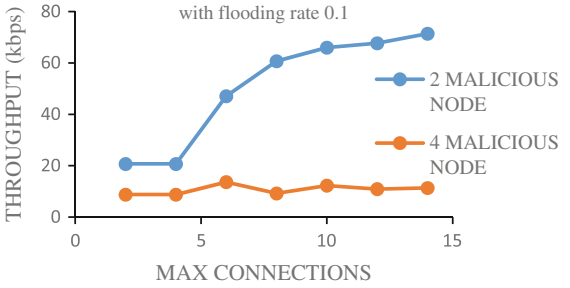

Fig. 4 Throughput versus maximum connection

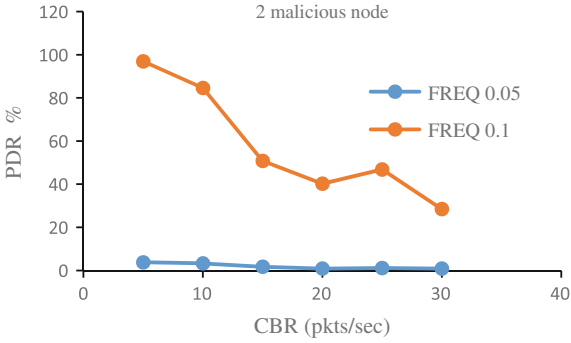

Fig. 5 PDR versus CBR rate

request flooding in the network. As shown at 10 packets per second CBR, PDR is 85 % for flooding rate 0.1 s and 4 % for 0.05 s.

Throughput over flooding rate (0.05, 0.1) with varying CBR rate: In Fig. 6 results shows on increasing CBR rate, throughput increases with increase in flooding rate. But with constant flooding rate, throughput increases with CBR rates due to flooding of request packet in the network. As shown at 10 CBR, throughput is 115 kbps for 0.1 flooding rate and 5 kbps for 0.05 flooding rate.

PDR over flooding rates (0.05, 0.1) with varying connections between nodes: In Fig. 7 results shows on increasing number of connection between nodes PDR increases with increase in flooding rate. As PDR is nearby 100 % for flooding rate 0.1 and 5 % for flooding rate 0.05 with increase in connection between nodes.

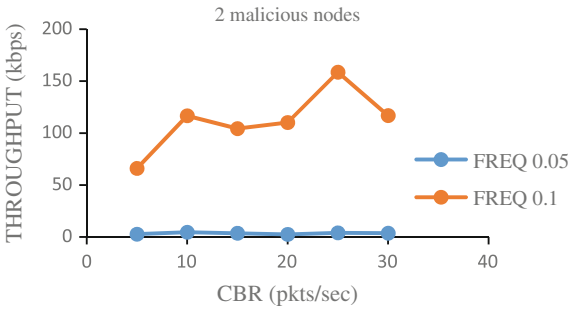

Fig. 6 Throughput versus CBR

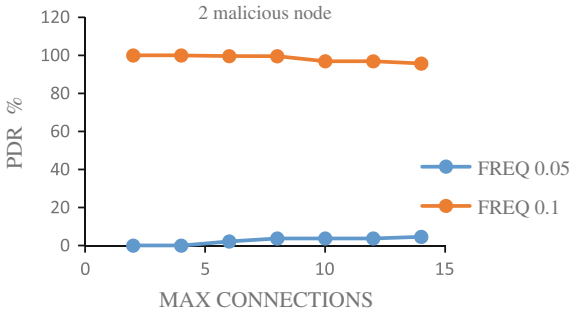

Fig. 7 PDR versus maximum connections

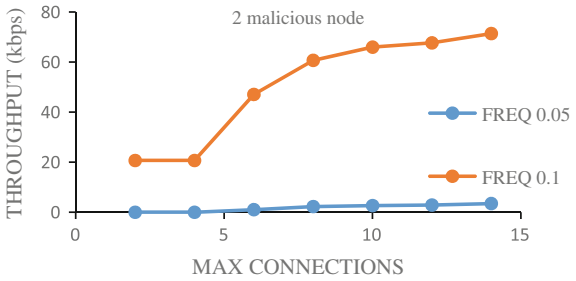

Fig. 8 Throughput versus maximum connections

Throughput over flooding rates (0.05, 0.1) with varying connections between nodes: Fig. 8 result shows on increasing connections between nodes throughput drastically increases with increase in flooding rate in presence of malicious nodes. As shown with 10 connections throughput is 3 kbps at 0.05 flooding rate and 66 kbps at 0.1 flooding rate in presence of 2 malicious nodes.

4 Conclusion

By identifying the impact of RREQ flooding attack on AODV routing protocol in MANET using NS2- network simulator, it was noticed that the presence of malicious flooding nodes can affect the performance of the overall wireless network as it introduces a fake route request and can act as one of the major security threat. From the simulation it can be concluded that due to the extensive flooding in the network average percentage of packet loss and bandwidth increases, which decreases packet delivery ratio and throughput with variable increase in parameters as speed, constant bit rate and connections between nodes. If flood nodes are more in number then there is drastic impact on the performance metrics of the routing protocol in the network. In future work, we will study and assess the effect of various types of attacks on MANET and further some novel security scheme will be proposed to detect and avoid any malicious nodes.

References

1. Wu, B., Chen, J., Wu, J., Cardei, M.: A survey on attacks and countermeasures in mobile ad hoc networks. In: Wireless/Mobile Network Security. Springer, Berlin (2008)
2. Bandyopadhyay, A., Vuppala, S., Choudhury, P.: A simulation analysis of flooding attack in MANET using NS-3. In: IEEE 2nd International Conference on Wireless VITAE (2011)
3. Ehsan, H., Khan, F.A.: Implementation and analysis of routing attacks in MANETs. In: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (2012)
4. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., Jamalipour, A.: A survey of routing attacks in mobile ad hoc networks. Proc. Wirel. Commun. IEEE **14**(5), 85–91 (2007)
5. Patel, M., Sharma, S.: Detection of malicious attack in MANET a behavioural approach. In: Advance Computing Conference (IACC), IEEE 3rd International (2013)
6. Corson, S., Macker, J.: Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations. Internet request for comment RFC 2501 (1999)
7. Perkins, C., Royer, E.M.: Ad hoc on demand distance vector (AODV) routing. Internet draft (1998)
8. Eu, Z., Seah, W.: Mitigating route request flooding attacks in mobile ad hoc networks. In: Proceedings of the International Conference on Information Networking (ICOIN'06), Sendai, Japan (2006)
9. Yi, P., Dai, Z., Zhong, Y., Zhang, S.: Resisting flooding attacks in ad hoc networks. In: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), pp. 657–662 (2005)
10. Verma, S.S., Patel, R.B., Lenka, S.K.: Investigating variable time flood request impact over QOS in MANET. In: 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)
11. Verma, S.S., Patel, R.B., Lenka, S.K.: Analyzing varying rate flood attack on real flow in MANET and solution proposal: real flow dynamic queue (RFDQ). Int. J. Inf. Commun. Technol. (in press) Inderscience, **7** (2015)
12. Shandilya, S.K., Sahu, S.: A trust based security scheme for RREQ flooding attack in MANET. Int. J. Comput. Appl., **5**(12), 4–8 (2010)
13. Ning, P., Sun, K.: How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols. Ad Hoc Netw. **3**(6), 795–819, Elsevier (2005)
14. Murphy, S., Yang, Y.: Generic threats to routing protocols. In: IETF RFC4593. Status Informational (2006)
15. Abolhasan, M., Wysocki, T., Dutkiewicz, E.: A review of routing protocols for mobile ad hoc networks. Technical report, Telecommunication and Information Research Institute, Australia (2003)
16. Fall, K., Varadhan, K.: NS manual. The VINT Project