Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPACT OF MISBEHAVIOR ON MODIFIED AODV PROTOCOL

[1]MANI P., [2]KAMALAKKANNAN P.

[1]Assistant Professor, Department of MCA, M. Kumarasamy College of Engineering, Karur, Tamilnadu, INDIA

[2]Assistant Professor, PG and Research Department of Computer Science, Government Arts College (Autonomous), Salem, Tamilnadu, INDIA

E-mail: [1]manimegalai.p@gmail.com , [2]kamal_karthi96@yahoo.co.in

ABSTRACT

Mobile Ad hoc Networks (MANETs) is a collection of mobile nodes forming the network dynamically for exchange of information using the multi-hop wireless communications. It is difficult to find the optimal route between source and destination due to the changing topology and dynamic nature of the mobile nodes. Routing protocols for mobile ad hoc networks are designed with an assumption that the nodes will cooperate in packet forwarding to establish communication between distant nodes using multi-hop communication. The cooperation between nodes does not exist always. In order to save scarce resources like battery power, bandwidth etc., the nodes may misbehave. A particular misbehavior, called malicious behavior, severely affects the performance of the ad hoc routing protocols. The malicious attack is carried out as a two phase attack launched by one or more malicious nodes. In the first phase, the malicious nodes try to lure legitimate node to send packets via them by participating in the network. In the second phase, these nodes drop all the data packets send via them thereby affecting the overall communication. In this paper, we have simulated the malicious behavior in Ad hoc On-demand Distance Vector (AODV) routing protocol using NS-2 and studied the impact of it on the performance of the mobile ad hoc networks with and without malicious behavior. The analysis was carried out using various metrics like packet delivery ratio, normalized routing load, average end-to-end delay and percentage of packet loss. Based on the analysis, we conclude that the steps have to be taken to thwart the malicious behavior otherwise it would be difficult to find routes longer than one or two hops.

Keywords: *Mobile Ad Hoc Networks, Malicious nodes, AODV, Malicious Behavior, NS-2*

1. INTRODUCTION

Mobile Ad Hoc Networks are the collection of mobile nodes which form the network on the move without the need for any fixed infrastructure. The mobile nodes act as hosts as well as router for exchange of information within the network. MANETs are used in various fields like crisis management and civilian applications. The crisis management includes deployment of mobile nodes in battle fields, emergency search and rescue and law enforcement where the nodes belong to a common authority and pursue a common goal is reported in [1] [2]. In the case of civilian applications, includes enabling communications among independent mobile nodes in conference halls, malls etc., and the nodes belong to different authority and does not have a common goal to pursue. All the routing protocols for manets are designed with an assumption that all the intermediate nodes are willing to forward the packets of other nodes. But this may not be true in all the cases. As an example, consider Figure 1 depicting a source S using a multi-hop path to route the packets to the destination D.

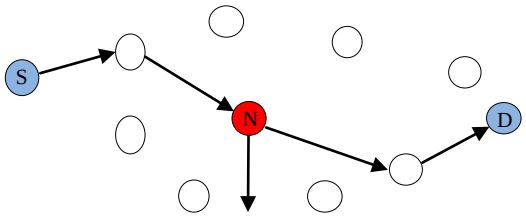

Figure 1: Misbehaving Node N Drops The Packets

This network model assumes that the intermediate nodes are willing to forward the packets other than their own. A protocol-compliant behavior cannot be assumed when an ad hoc network deployed in a hostile environment. In order to save the limited resources like energy, the node may not forward the packets of other nodes. Nodes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

exhibiting such behavior are termed as selfish. The selfish nodes are rational that they do not disrupt the network operation but still they want to use the services of other nodes to send and receive their own packets. The other kind of misbehavior called malicious behavior which disrupts the network operations. In general, the presence of misbehaving nodes in the network will degrade the network performance abruptly.

Inherent characteristics of MANETs, like no fixed infrastructure, wireless medium and dynamic topology, introduces various security attacks as discussed in [3]. These attacks can be broadly classified into two categories namely passive and active attacks. In passive attacks, the misbehaving nodes do not disturb the operation of the network, but it collects the needed information about the network since it is very difficult to find out the passive attack. An active attack disturbs the operation of the network and can further be classified into internal attacks and external attacks. The internal attacks are launched by the nodes which are part of the network whereas the external attacks are launched by the nodes which are not part of the network.

1.1 Security Requirements

1.1.1 Confidentiality

The network should ensure that the given message cannot be understood by anyone other than its recipients. It can be enabled by cryptographic technique.

1.1.2 Authentication

The network should ensure that the data is send and received by the authenticated user only.

1.1.3 Non-Repudiation

It is the ability of the network to ensure that a node cannot deny the sending of a message that it originated.

1.1.4 Availability

The network should provide the required services to the authenticated users when it is expected.

1.1.5 Integrity

The system should ensure that the message sent from the sender is received by the receiver without any modification during transmission.

The main functions of the network layer are routing and forwarding. The malicious behavior at the network layer can be created by modifying the ad hoc routing protocols. The aim of this paper is to simulate the malicious behavior in AODV using ns-2 and analyze the impact on network performance. Even though ns-2 contains AODV routing protocol, it does not have any modules to simulate malicious behavior. So we have modified the source code to exhibit malicious behavior. Having implemented the malicious behavior, we performed simulation on different scenarios to compare the network performance with and without malicious behavior in the network based on various parameters like packet delivery fraction, packet loss, average end-to-end delay and normalized routing load.

2. RELATED WORKS

The authors in [4] [5] surveyed the various attacks on mobile ad hoc networks. They have listed out the research works carried out by many researchers to prevent and detect the misbehavior in order to improve the performance of the network. The main assumption of the MANET routing protocols is that all participating mobile nodes do so in good faith and without maliciously disrupting the operation of the protocol [6]. The study of malicious behavior and its impact on the network performance is very essential to understand and to develop a robust routing protocol which guards the network against various attacks. The first work on misbehavior has been implemented by [7]. They have proposed a method for categorizing nodes based upon their dynamically measured behavior. The authors have introduced two extensions to the Dynamic Source Routing [8] to mitigate the effects of routing misbehavior: The watchdog and the pathrater. The watchdog indentifies misbehaving nodes by listening in the promiscuous mode, while the pathrater avoids routing packets through these nodes.

The watchdog mechanism is implemented on top of DSR by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed otherwise it determines that the node is misbehaving. The watchdog mechanism works well on top of the source routing protocol. The main drawback of this method is that it may not detect misbehaving nodes in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior collusion and partial dropping.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The rest of the paper is organized as follows: Section 2 presents the classification of various ad hoc routing protocols. Section 3 gives an overview of AODV protocol. Section 4 describes the proposed scheme, Section 5 presents the experimental results and Section 6 concludes the paper and outlines future work.

3. CLASSIFICATION OF ROUTING PROTOCOLS

The routing protocols for ad hoc networks can be classified into different types based on routing information update mechanism, use of temporal information for routing and topology of information organization etc., as given by [9]. Based on the routing information update mechanism, the routing protocols can be classified into proactive or table driven routing protocols, reactive or on-demand routing protocols and hybrid routing protocols as in [10].

3.1 Table-driven Routing Protocols

In proactive or table-driven routing protocols, each node maintains up-to-date routing information in the form of routing tables by periodically exchanging routing information and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The examples of proactive routing protocol include Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Cluster-head Gateway Switch Routing Protocol (CGSR), Source-tree Adaptive Routing Protocol (STAR), Fish-eye State Routing (FSR), Optimized Link State Routing (OLSR) Hierarchical State Routing (HSR) and Global State Routing (GSR).

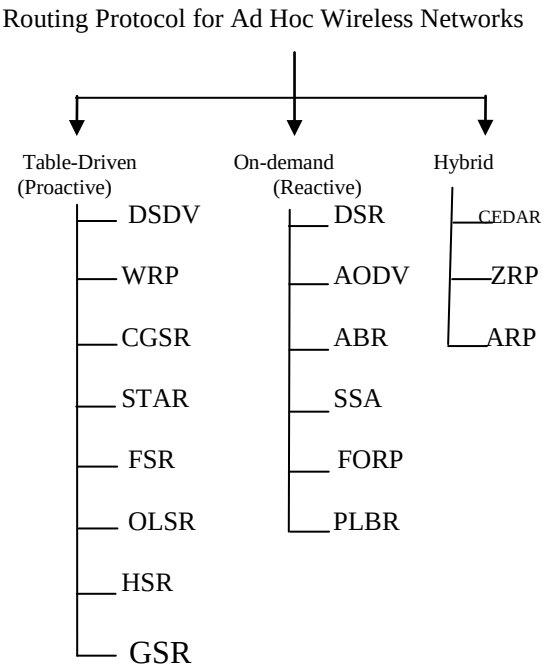

Figure 2: Classification of Routing Protocols

3.2 On-demand Routing Protocols

The on-demand routing protocols execute the path-finding process and exchange routing information only when a path is required by a node to communicate with a destination. This kind of protocols is usually based on flooding the network with Route REQuest (RREQ) and Route REPly (RREP) messages. The route is discovered from source to destination node with the help of route request messages. The destination node establishes the route path by sending RREP messages. Some of the on-demand ad hoc routing protocols are Dynamic source Routing (DSR), Ad hoc On-demand Distance Vector (AODV), Associativity Based Routing (ABR), Signal Stability-based Adaptive Routing (SSA) and Flow-Oriented Routing Protocol (FORP) and Preferred Link State Routing (PLBR).

3.3 Hybrid Routing Protocols

The proactive and reactive protocol each works best in different scenarios, hybrid protocol uses both. It is used to find the balance between both protocols. Examples of hybrid routing protocols are Core Extraction Distributed Ad Hoc Routing (CEDAR), Zone Routing Protocol (ZRP) and Wireless Ad Hoc Routing Protocol (WARP).

Journal of Theoretical and Applied Information Technology
30th November 2013. Vol. 57 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. OVERVIEW OF AODV

The author [6] proposed an on-demand approach for finding routes, i.e., a route is established only when it is required by a source node for transmitting data packets. The source node floods the Route REQuest (RREQ) packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single RREQ. The major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number to determine an up-to-date path to the destination. A node updates its path information only if the destination sequence number of the current packet received is greater that the last destination sequence number at the node.

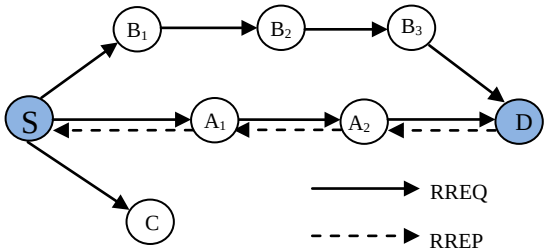

Figure 3: Route Discovery in AODV

When an intermediate node receives a RREQ it either forwards it or prepares a Route REPly (RREP) if it has valid route to the destination. The validity of the route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RREQ packet. If a RREQ is received multiple times, the duplicate copies are discarded. All intermediate nodes having valid route to the destination are allowed to send RREP packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.

When a path breaks, the nodes at both the ends initiates the RouteError messages to inform their end nodes about the link break. The end nodes delete the corresponding entries from their tables. The source node reinitiates the path-finding process.

5. PROPOSED SCHEME

In many civilian applications the nodes does not belong to a single authority and do not have a common goal. In such networks, forwarding packets for others is not in the direct interest of nodes, so there is no good reason to trust nodes and assume that they always cooperate. Indeed, a selfish node may try to preserve its resource. The malicious behavior disturbs other nodes and its intention is not to save its resources. The malicious behavior has been simulated using AODV routing protocol. When a packet is received by AODV protocol, it processes the packets based on its type. If the received packet is a data packet, normally AODV protocol sends it to the destination address, but behaving as a malicious node it drops all data packets. Whenever the malicious node receives an RREQ packet it immediately sends RREP packet as if it has fresh enough path to the destination. Malicious node tries to deceive nodes by sending such an RREP packet with highest sequence number of AODV protocol and low hop count. The detailed study of the paper helps in determining the vulnerability of the ad-hoc routing protocols so that they can be made more robust.

Algorithm
Begin
Modify the AODV protocol to include malicious behavior
Node initialization
Randomly deploy malicious nodes in the network
Start the network operation
//On receiving RREQ, malicious node do the following
If (node itself is destination or node is intermediate node)
begin
Send the RREP with highest sequence number and low hop count to the source node
end
Source node selects the route with highest sequence number and starts transmitting packets
If (node is malicious)
begin
Drops all data packets
end
end

6. PERFORMANCE EVALUATION

6.1 Simulation Environment

Every protocol is having its own advantages and disadvantages, none of them can be claimed as absolutely better than others. To study the impact of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

malicious behavior on network performance, we have selected the AODV for evaluation.

The simulation was carried out using NS 2.34 [11]. The traffic sources are Constant Bit Rate (CBR). The source and destination pairs are spread randomly over the network area. The mobility model uses the random waypoint model in a rectangular field of 1000m x 1000m by varying the number of nodes. During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes a rest period of time in seconds and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. The malicious behavior is added to the source codes to analyze the performance of AODV with malicious behavior. 20% of the nodes are chosen randomly as malicious nodes which drop all the packets forwarded through them. The results of the AODV with and without malicious nodes are compared to measure the performance of the network.

The simulation parameters are listed in the Table.

Table 1: Simulation Parameters

Parameter	Value	Description
Simulation time	100 s	Simulation time
Traffic Type	CBR	Constant Bit Rate
Number of nodes	10,20,30,40 and 50	Number of nodes
Area of the network	1000m x 1000m	Area of the network
Queue Length	50	Queue Size
Transmission Range	250m	Transmission Range
Mobility Model	Random waypoint	Mobility Model

6.2 Performance Metrics Used

We used the following metrics to measure the impact of misbehavior on network performance using AODV with and without malicious behavior.

6.2.1 Packet Delivery Fraction

It is defined as the total number of packets successfully received at the destination to the total number of packets generated by the source.

6.2.2 Normalized Routing Load

The number of routing packets transmitted per data packet delivered at the destination. Each hop – wise transmission of a routing packet is counted as one transmission.

6.2.3 Average End-to-end Delay

This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer time.

6.2.4 Packet Loss

It is defined as the ratio between number of packets generated by the source to the number of packets successfully received.

6.3 Simulation Results

We have conducted simulations by varying the number of mobile nodes while keeping the number of malicious nodes same. The simulations were repeated for five times for each scenario to get an average data point.

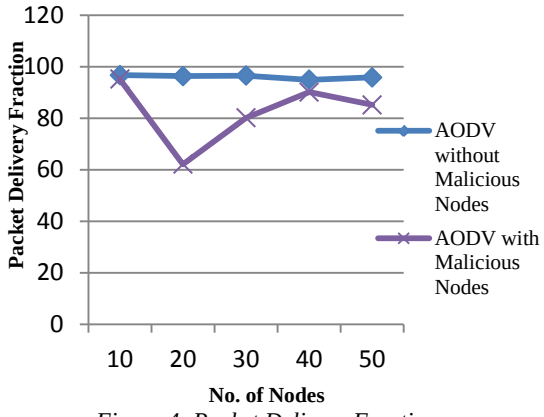

Figure 4: Packet Delivery Fraction

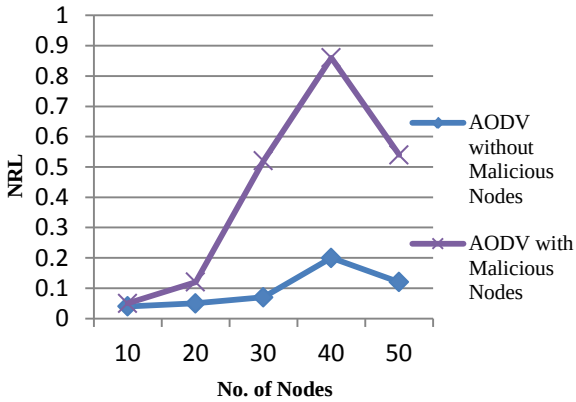

Figure 5: Normalized Routing Load

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

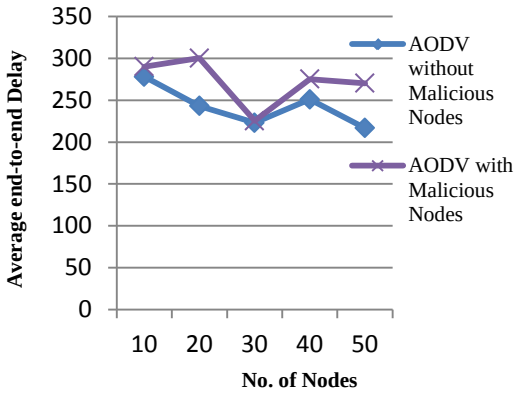

Figure 6: Average end-to-end Delay

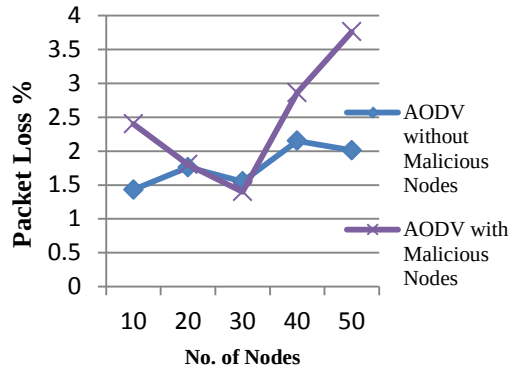

Figure 7: Packet Loss %

We compared the results with and without the presence of malicious behavior in mobile ad hoc networks. The route path from source to destination is established through route discovery process. If any malicious node is included in the route path, it drops all the data packets forwarded through them. So it affects the data forwarding process thereby brings down the communication in the network. The position and number of malicious nodes have significantly deteriorated the network performance. The parameters like packet delivery fraction, packet loss, average end-to-end delay and normalized routing load have been analysed and the result shows that the some measures have to be taken to mitigate the malicious behavior as it affects the communication in the mobile ad hoc networks.

7. CONCLUSION

The malicious behavior in mobile ad hoc networks can severely deteriorate the network performance and weakening the security enhancements. In this paper, we have simulated the malicious behavior in AODV routing protocol of mobile ad hoc networks and studied its impact on network performance with and without malicious behavior. The parameters like packet delivery fraction, packet loss, average end-to-end delay and normalized routing load have been analyzed. This will help us to build more robust routing protocols against this kind of attack. As a future work, this could be extended to simulate the malicious behavior with respect to other ad hoc routing protocols to analyze the impact on network performance with and without malicious nodes.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their comments and suggestions.

REFERENCES

[1] Merwe J.V.D., Dawoud D., and Mcdonald S., "A survey on peer-to-peer key management for mobile ad hoc networks," *ACM Computing Surveys*, vol. 39, no. 1, pp. 1 - 45, 2007.

[2] Y Zhang, W Liu, W Lou, and Y Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Transactions on Dependable and Secure computing*, vol. 3, pp. 386 - 399, 2006.

[3] Hongmei D, Wei L, and D.P. Agarwal, "Routing Security in Wireless Ad Hoc Networks," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 70-75, October 2002.

[4] S. Djahel, F. Nait- Abdesselam, and Z. Zhang, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, Fourth Quarter 2011.

[5] Mani P. and Kamalakkannan P., "Mitigating Selfish Behavior in Mobile Ad Hoc Networks - A Survey," *International Journal of Computer Applications*, vol. 73, no. 22, pp. 1 - 7, July 2013.

[6] C.E. Perkins, E.M. Royer, and S.R. Das, "Ad Hoc on-demand Distance Vector(AODV) Routing," IETF MANET Working Group, draft-ietf-manet-aodv-10.txt, 2002.

[7] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in *In proc. 6th annual international conference on Mobile Computing and Networking (MOBICOM '00)*, Boston, Massachusetts, August 2000, pp. 255-265.

[8] D.B. Johnson and D.A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft)," Mobile Ad Hoc

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Network (MANET) Working Group, IETF, 2004.

[9] C. Siva Ram Murthy and B.S. Manoj, *Ad Hoc Wireless Networks Architectures and Protocols*. New Delhi, India: PearsonEducation, Inc.

[10] Mehran Abolhasan, Tadeusz Wysockia , and Eryk Dutkiewicz , "A review of routing protocols for mobile ad hoc networks," *Ad Hoc Networks*, vol. 2, no. 1, pp. 1 - 22, 2004.

[11] [Online]. http://www.isi.edu/nsam/ns