Performance Evaluation of Malicious node in Mobile Ad Hoc Network using AODV Protocol

Vivek Richhriya
Professor, CSE, LNCT, Bhopal

Jay Prakash Maurya
Asst.Professor, CSE, LNCT, Bhopal

Tripti Saxena
Asst. Professor Professor, CSE, LNCT, Bhopal

ABSTRACT *MANETs (Mobile Ad hoc Network) is collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. The routing is the one of the prime requirement. MANETs function work properly only if the participating node do not show misbehavior (selfishness) and play their role in routing & forwarding the packets. Due to nature of mobility, the transmission range of node is limited & the normal operation of network is disturbed by malicious node. Since AODV does not comprise any particular security methods, such as strong authentication, etc. Hence, there is no clear-cut method to prevent mischievous behavior of a node in AODV protocol. The main objective of this paper is to analyze the performance of AODV in the presence of malicious nodes with the help of NS-2.*

KEYWORDS *AODV, Malicious Nodes, Security, MANET, NS2*

1. INTRODUCTION

Security is prime and main issue in MANET. There is no specific security features defined in AODV. Therefore animpersonation attack can be easily made. A node is called *malicious* if it is an attacker that cannot validate itself as alegitimate node due to the lack of valid cryptographicinformation [1]. A node is called *compromised* if it is an inside attackerwhich is acting maliciously but can be authenticated by thenetwork as a legitimate node and is being trusted by other nodes. There are severalattacks that can be founded against the AODV routingprotocol as follows [2].

- *Message dropping attack*: Malicious or selfish nodes deliberately drop all packets that are not destined for them. The mainaim of malicious nodes is to disrupt the network connection where as selfish nodesaim to maintain their resources. Message dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a decisive point. It also reduces the network performance by causing data packets to be retransmitted and new routes to the destination to be detected.This attack can paralyze the network entirely as the number of message dropping increments [3].
- *Wormhole attack* (*Message replay*) :An attacker receives packets at one location and tunnels them to another location in the same network. As the result off,routing can be disrupted when routing control messages are tunneled. Due to this, tunnel between two colluding attackers is known as a wormhole. Theseattacks are severe threats to MANET routing protocols. For example, when a wormhole attack is applied against an on-demand routing protocol (such as AODV or DSR), the attack could prevent the discovery of any routes other than through the wormhole [2,3].
- *Message tampering attack*: An attacker can modify the content of routing messages and forward them with falsified information. Insider attackers modify packets to disrupt the network. Since nodes in the ad hoc networks are free to move and self-organize & self motivated, relationships among nodes at some times might include the malicious nodes. These malicious nodes may exploit the periodic relationships in the network and later launch the message modification attacks. The types of attacks under the message modification attacks are impersonation attacks and packet misrouting [3,1].

2. RELATED WORK

Since AODV does not comprise any specific security mechanism, such as strong authentication. Hence, there is no straightforward method to prevent mischievous behavior of a node in AODV protocol. However AODV protocol stillhas many weaknesses. Due to this, many researchers todevelop new variants protocol based on AODV toimprove its performance [4].An enhancement to the AODV protocol is presented by [5] to avoid black-hole attacks called DPRAODV. According to this proposed solution the requesting node without sending the DATA packets to the reply node at once, has to wait till other replies with next hop details from the other neighbouring nodes. Hence, the mobile node, which is battery-powered, has to wait sometime before a safe path isdiscovered which will consume the batterypower. It [6] proposed a game theoretic approach called AODV-Game Theoretic (AODV-GT) and we integrate this into the reactive AODV to provide defence against black-hole attacks. AODV-GT is based on the concept of non-cooperative game theory. [7] have presented a hierarchical secure routing protocol (HSRBH) for detecting and defending against black-hole attacks. It uses symmetric key cryptography to discover a safe route against the attacks. However sharing a key among user's can be risky.

3. OVERVIEW OF AODV

AODV is on demand routing protocol & a variation of Destination-SequencedDistance-Vector(DSDV) routing protocol which is cooperatively based on DSR and DSDV. In AODV, routes are only established when needed. AODV supports Unicasting&Multicasting within a uniform framework [8]. The Count-To-Infinity and loop problem areremovedby using destinationsequence numbers and the registration of the costs. Every hop has the constant cost of one.

Route Discovery:

When a sendernode wants to send a data packet to a destination node in the network, the source node searches its route table for a route to destination. If there is a route,data packet is forwarded to the appropriate next hop toward thedestination. If it is not, the route discovery process is started. AODV initiates a route discovery process with the help of RouteRequest (RREQ) and Route Reply (RREP). First, the source nodewill create a RREQ packet that contains broadcast ID,its current sequence number, its IP address, the destination's IP address, and the destination'slast sequence number. Broadcast ID is incremented each time when source node initiates RREQ. The sequence numbers are used to an up-to-date path to a destination [9]. Every details in the route table is associated with a sequence number. The pair of broadcast ID & the IPaddress makes a unique identifier for RREQ thus as touniquely identify each request. The source nodebroadcasts the RREQ packet to its intermediate neighbors and then sets atimer to wait for a reply. In order to process the RREQ, the node createsa reverse route entry for the source node in its routing table. A node can send a RREP (Route Reply packet) to the source using the reverse route [10].

Setting up of Forward Path:

When the destination node or an intermediate node receives the RREQ with a route to the destination, it creates the RREP and then unicast the same towards the source node. The reverse path will be used for sending a RREP message i.e. this forward path is reverse to the reverse path. As RREP isrouted back along the reverse path and also received by anintermediate node, it creates a forward path entry to thedestination in its route table. At the last, when the RREP reaches thesource node, it means that a route from source to the destination hasbeen established and now the source node can start the datatransmission [8].

Route Maintenance:

A route discovered between a source node and destination nodeis preserved as long as required by the source node. As thereis movement of nodes in MANETs and if thesource node moves during data transmission, it can reinitiateroute discovery mechanism to find out a new route todestination. On the other hand, if the destination node or someintermediate node displaces, the Route Error (RERR) message is sent to its just intermediate node. As a result, these nodes propagatethe RERR to their predecessor nodes. In this way, this process continuesuntil the source node is reached. As RERR is received by thesource node, then it can either stop sending the data or reinitiate theroute discovery process by sending a new RREQ message ifthe route is still needed [10].

Merits and Limitations:

The merits of AODV protocol are as follows [8,9]:

- The routes are established when needed and destinationsequence numbers are used to find out the latest route to thedestination.
- It supports both unicasting and multicasting packettransmission.
- It also responds very speedily to the topological changes thataffects the active routes.
- Itreduce the control traffic messages overhead.

The limitations of AODV protocol are given below:

- The performance of AODV protocol without any selfish or malicious nodes is poor in large network.
- It can gather only avery limited routing information, route learning is limited only for any routing packets being forwarded by source node.
- Due to multiple Route Reply packets in response to a singleRoute Request packet can lead to heavy control overhead.As the result periodic beaconing leads to unnecessary bandwidthconsumption.
- It is defenseless to various kinds of attacks as it isassumed that all nodes must cooperate and without theircooperation no route can be set up.

4. ROLE OF MALICIOUS NODES IN AODV

The attacker or malicious node usually exploits some routing protocols to distribute itself as having the direct and shorter route to source whose packets it wants to grab [11]. Once the attacker adds itself between the communicating nodes, it can do anything malicious with the packets passing between them. It can then choose to drop the packets thereby creating Denial of Service attacks. Security in mobile ad-hoc network is the most vital concern for basic functionality of a network [12].

The work done in earlier years based on security issues i.e. attacks (particularly Black hole) on MANETs is mainly based on reactive routing protocols like Ad-Hoc on Demand Distance Vector (AODV) [11]. Black hole attack has been reviewed and its effects have been analyzed by studying how these attacks disturb the performance of an ad hoc network. A very little attention has been given on the impact of Black hole attack on routing protocols and comparison of vulnerability of these protocols against the attacks [13]. The goal of this work is to study the effects of Black hole attacks on reactive routing protocols i.e. Ad-Hoc on Demand Distance Vector (AODV).The malicious nodes attack is the type of messagedropping attack in which attack is performed on every route request, rote reply ordata packet by the malicious nodes [14].

In order to introduce malicious nodes in AODV,first we need to modify aodv.cc and aodv.h files:

In aodv.h:

```
        bool malicious;
```

In aodv.cc:

```
        malicious = false;
        if(strcmp(argv[1], "hacker") == 0) {
        malicious = true;
        return TCL_OK; }
```

Next we need to modify the TCL file to set a malicious node:

```
    $ns at 0.0 "[$mnode_(i) set ragent_] hacker"
if (malicious == true ) {
drop (p,DROP_RTR_ROUTE_LOOP); }
```

5. SIMULATION SETUP AND RESULTS

The performance study of malicious node has been done in AODV using NS-2 simulator. In order to measures the performance evaluation different metrics like Packet Delivery Ratio, End to end delay and Throughput, has been used. In all these cases the number of malicious node varies from 0 to 5.

Parameter	Value
Number of Nodes	50
Routing Protocol	AODV

Maximum mobility speed of nodes	CBR
Communication Type	10 m/sec.
Simulation Area	1000m x 1000 m
Simulation Time	250 sec
Number of malicious nodes	0, 1, 2, 3, 4, 5
Packet Sizes	512bytes

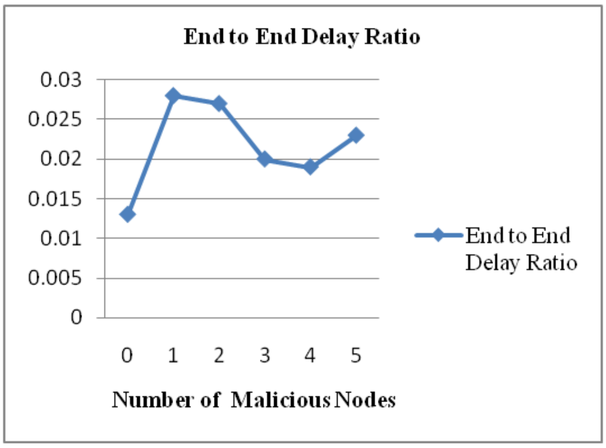

Figure 1: End to End Delay Ratio V/s Number of Malicious Nodes

Figure 1 shows end to end delay ratio. End to end delay ratio should be less in wireless network. In this figure end to end delay ratio are calculated with different scenarios varying using the number of malicious nodes. The “0” malicious node shows the minimum end to end delay ratio i.e. 0.01312 and after that end to end delay ratio is high in comparison to “0” malicious node which vary from 0224 to 02887.

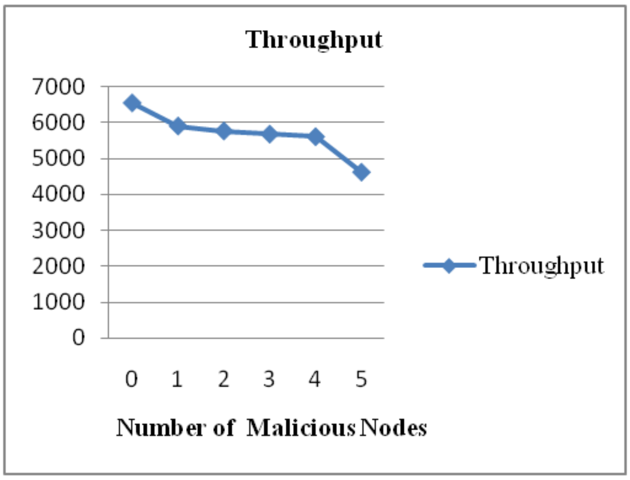

Figure 2: Throughput V/s Number of Malicious Nodes

Figure 2 shows that how many control packets are dropped. In these control packets included route request, route reply and route error, the control packets dropped vary with the number of malicious nodes. The “0” define that there is no malicious node in AODV and control packets dropped is only 1. With malicious nodes 1 to 4 control packets dropped is high in comparison to without malicious node i.e. 94 to 106. But with 5 malicious nodes control packets dropped is very high in comparison to the other scenarios i.e. 228.

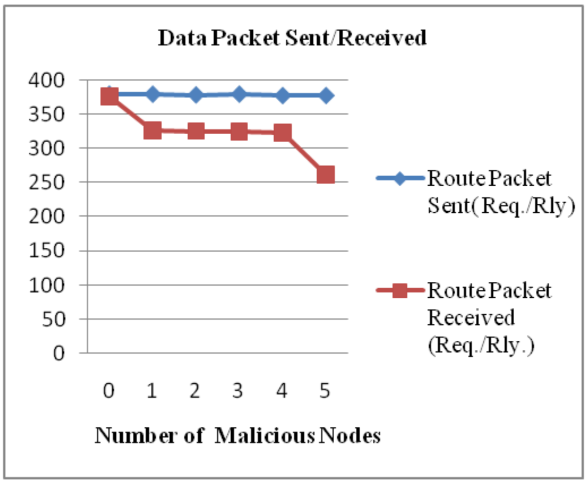

Figure 3: Data Packets Sent / Received V/s Number of Malicious Nodes

Figure 3 shows that how many data packets are sent and received. Data packets received different number of malicious nodes. The “0” define that there is no malicious node in AODV and data sent / data received is excellent i.e. 380 / 377 which shows that in this scenario only 3 data packet is dropped. With malicious nodes 1 to 4 the data received is 324 to 327 which are less than “0” malicious node results. But with 5 malicious nodes data received is very less than to the without malicious node scenario i.e. 262.

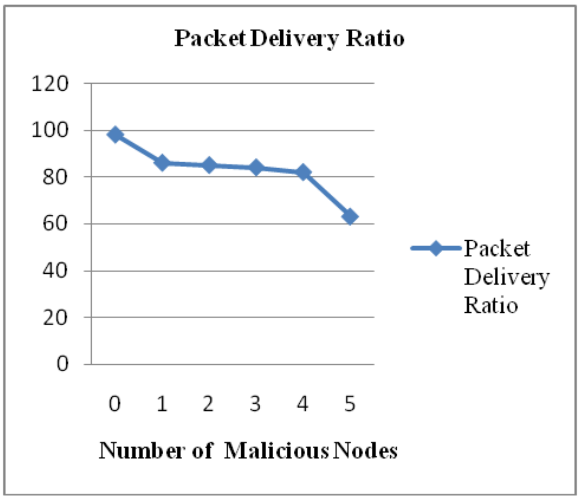

Figure 4: PDR V/s Number of Malicious Nodes

Figure 4 shows the packet delivery ratio with varying thenumber of malicious nodes. The “0” define that there is no maliciousnode in AODV and PDR is excellent i.e. 99.67%. Withmalicious nodes 1 to 4 PDR is less compare to withoutmalicious node i.e. 84.15% TO 84.89%. But with 5 maliciousnodes PDR is very less in comparison to the without maliciousnode scenario i.e. 68.19 (which around 30% less).

6. CONCLUSION AND FUTURE WORK

In this paper, all the results that show malicious nodes in the network give a badimpact on the performance of AODV in terms ofthroughput, packet delivery ratio, datapacket sent / receive and end to end delay ratio.In this paper, we explain only malicious attacks simulate and analyze theresults but there is no methods are used to detect and preventmalicious nodes in AODV. For future work, an effortwill be used to detect and prevent the working of maliciousnode from the AODV.

REFERENCES

[1] S.Gopinath1, Dr.S.Nirmala & N.Sureshkumar, "Misbehavior Detection: A New Approach for MANET",(IJERA) ISSN: 2248-9622 www.ijera.com,Vol. 2, Issue 1,Jan-Feb 2012, pp.993-997.

[2] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei, “A Survey on Attack and countermeasures in Mobile Ad Hoc Network”, Springer 2006.

[3] Qi Zhang and Dharma P. Agrawal, “Impact of Selfish Nodes on Route Discovery in Mobile Ad Hoc Networks”,IEEE Communications Society, pp. 2914-2918, 2004.

[4] Datuk Prof IrIshak Ismail &MohdHairilFitriJa’afar,"Mobile Ad Hoc Network Overview", Asia-Pacific Conference On Applied Electromagnetics Proceedings, 2007.

[5] Payal N. Raj, Prashant B. Swadas, “DPRAODV: A Dyanamic Learning System AgainstBlackhole Attack In Bodv Based Manet”, In: International Journal of Computer Science Issues, Vol.2, pp 54- 59, 2009.

[6] Panaousis A. E., Politis, C.: A Game Theoretic Approach for Securing AODV in Emergency Mobile Ad Hoc Networks. In: IEEE 34th Conference on LocalComputer Networks (LCN 2009), pp. 985- -992, Zurich, Switzerland (2009).

[7] Yin, J., Madria, S.: A Hierarchical Secure Routing Protocol against Black hole Attacks in Sensor Networks. In: IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 8, Taichung, Taiwan (2006).

[8] AODV homepage. http://moment.cs.ucsb.edu/aodv/aodv.html

[9] Ye Tung; Alkhatib, M.; Rahman, Q.S.,"Security Issues in Ad-Hoc on Demand Distance Vector Routing (AODV) in Mobile Ad-Hoc Networks", Proceedings of the IEEE , vol., no., pp.339-340, 2005.

[10] Royer E.M. Perkins C.E. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, p.90, 1999.

[11] Tamilselvan, L., Sankarnarayanan, V.: Prevention of Blackhole Attack in MANET. In: 2nd International Conference on Wireless Broadband and Ultraband Communications, pp. 21, Sydney, Australia (2007)

[12] LoayAbusalah, AshfaqKhokhar, and Mohsen Guizani, “A Survey ofSecure Mobile Ad Hoc Routing Protocols”, IEEE communicationssurveys & tutorials, Vol. 10, no. 4, pp. 78- 93, 2008.

[13] Vijay Kumar and Ashwani Kush, “ Detection and Recovery of Malicious Node in Mobile Ad Hoc Networks”, International Journal of Advanced Research in Computer Science and Software Engineering , ISSN: 2277 128X, Volume 2, Issue 1, January 2012.

[14] K. Biswas and Md. Liaqat Ali, ―Security threats in Mobile Ad-Hoc Network‖ , Master Thesis, Blekinge Institute of Technology‖ Sweden, 22nd March 2007.

[15] Schiller J. Mobile Communications. Addison Wesley, 2nd edition, 2003.