Performance of AODV against Malicious node in Mobile Ad Hoc Network

Vivek Richhriya
Professor, CSE LNCT, Bhopal

Vineet Richhriya
Asst. Professor LNCT, Bhopal

Jay Prakash Maurya
Asst. Professor LNCT, Bhopal

ABSTRACT- *MANETs (Mobile Ad hoc Network) is collection of wireless nodes that can move anywhere and formof dynamically network without using pre-fix network administration . 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 having any particular security methods, e.g. strong authentication. 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.*

Key Words: *AODV, Malicious Nodes, Security, MANET, NS2*

I. INTRODUCTION

MANETs (Mobile Ad hoc Network) is collection of wireless nodes that can move anywhere and form of dynamically network without using pre-fix network administration. Due to this each & every node play a role of router. If the wireless nodes are within the range of each other, no routing is required. But if nodes moves out of this range and are able to communicate with each other directly, then we have to rely on intermediate node that organize the network and take the responsibility of data transmission. For this purpose, we need the routing algorithm to define the process of transmitting the packets from source to destination. During data transmission, security is prime and main issue in MANET. There is no specific security features defined in AODV. Therefore animpersonation attack can be possible and easily made by attackers. A node is called *malicious* if they try to attempt to bring down network connectivity by acting to be cooperative [2]. A node is called *compromised* if it is an inside attackerwhich is acting maliciously but can be authenticated by thenetwork as authenticate node and is being relied by other nodes in the network. There are severalattacks that can be founded against the AODV routingprotocol as follows [3,4].

• *Message dropping attack*: Malicious or selfish nodes intentionally drop all packets that are not intended for them. The mainaim of malicious nodes is to disrupt the network connection where as selfish nodesaim to maintain their resources.Thisattacks can foreclose end-to-end communications between mobile nodes in the network, if the dropping node is at a decisive point. It also brings down the performance of the network by causing data packets to be retransmitted and new routes to the destination to be detected.Due to this reason, the network can paralyze entirely as the number of message dropping increments.

• *Message replayAttack* :An attacker receives packets at one location and tunnels them to another location in the same network. As the result off,routing can be interrupted when routing control messages are tunneled. Due to this, tunnel between two colluding attackers is called as a wormhole. Theseattacks are terriblemenaces to MANET routing protocols. For example, when a wormhole attack is applied against an on-demand routing protocol, it could prevent the search of any routes other than through the wormhole.

• *Message tampering attack*: An attacker can modify the content of routing messages and forward them with falsified information. Insider attackers may modify data packets to interrupt the network. Since nodes in the MANETs are free to move,self motivated, self-organize and relationships among nodes at some times might include the malicious nodes. Due to this, malicious nodes may feat the periodic relationships later onestablish the message modification attacks. The types of the message modification attacks are also referred as impersonation attacks and packet misrouting.

The remainder of the paper is organized as follows. Section II provides related works in the node cooperation in MANETAS using reputation approach.Overview of the AODV protocol is presented in Section III. The detailed description of our proposed work are presented in Section IV, followed by the simulation results in Section V. Then, the conclusion in drawn in Section VI.

II. RELATED WORK

Standard Recently, alotofresearchhasfocusedonthecooperation issueinMANET. Several relatedissuesarebrieflypresentedhere.

BucheggerandLe Boudec[5] present the CONFIDANT protocol. CONFIDANT deals with not only the selfish but also several types of misbehavior such as silent route change or frequent route updates. Each nodemonitor the behavior ofitsnexthopneighborsinasimilarmannertowatchdog. But decidingthecriteriafor maintainingthefriendslistbyTrustManagerisdifficult.Bansaletal[6]haveproposeda protocolcalledOCEAN(Observation-basedCooperation EnforcementinAdhocNetworks),whichistheenhancedversionofDSRprotocol. Each node maintain the ratings for neighbor who directly interact with it. These ratings are not propagated to any other node. Due to this,OCEANfailsto deal with misbehaving nodes properly.CORE(Collaborative Reputation)[7]isareputationbasedsystemproposedbyMichiardietal similartoCONFIDANT and aims to detect and

Published By:
International Journal of Engineering Research in Current Trends

isolate selfish nodes.The node reputation is heavily weighted towards past reputation, therefore, cooperative node with low battery condition would not be detected as misbehaving nodes right away. The limitationwithCOREis thatthemostreputednodesmaybecome congested asmost ofthe routes arelikely topass through them. KhairulAzmietal[8]presenta newmechanismtodetectselfishnode.Eachnodeisexpectedto contribute tothe network on the continual basis within atime frame. Those which fail willundergo atestfortheirsuspicious behavior. Thisschemeisalsoabasedonmonitor node. A monitoring node hearsarequestfromitsneighbouringnodetoforwarda datapacket;itwillfirst check the time difference between *last request* and *last action* and status of the requestor. Misbehaviordetection andreactionaredescribed in[9],byMarti,Giuli,LaiandBaker.The paper presents two extensions to the DSR algorithm: the watchdog and the path rater. The watchdogidentifiesmisbehavingnodesbylisteningpromiscuouslytothenextnodetransmission butnotdetectmisbehaviorin presenceofambiguouscollisions,receivercollisions,limited transmissionpower,falsemisbehaviorandpartialdropping.

III. OVERVIEW OF AODV PROTOCOL

Since AODV does not having any particular security methods, e.g. strong authentication. Hence, there is no direct method to foreclose mischievous activity of a node in AODV protocol. However AODV protocol stillhas many weaknesses. Due to this, many investigators toformulate new forms protocol based on AODV tobetter its performance [10].

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 protocol, routes are only set up when needed. AODV supports Unicasting&Multicasting within a uniform framework [4]. The Count-To-Infinity and loop problem areremovedby using destinationsequence numbers and the registration of the costs.Having the constant cost of one of every hop in AODV.

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 [11]. 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. 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.

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 [11].

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.

IV. PROPOSED WORK

WeproposedanIDSsystemforidentifyingmalicious node under the BlackHoleattack usingAODV protocolwithCBRtraffic. MostoftheBlackHoleattacks areinvisible inthesystemand silently dropsthepacketsfromtheincoming trafficwithout sendingthemessagetothesendernodethatthepacketshave been dropped. The Flow chart of our proposed IDE is given below and also defined simulation parameters.

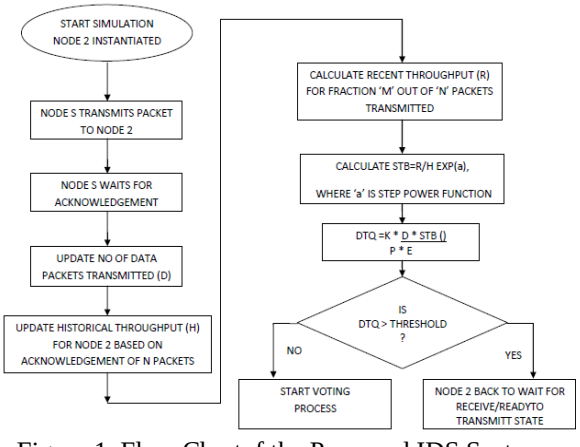

Figure:1. Flow Chartof the Proposed IDS System.

The simulation parameters, we defined as follows

$$STB(\quad) = \frac{R}{H}\, EXP(a)$$

$$DTQ = K * \frac{D * STB(\,)}{P * E}$$

$$DTE > THRESHOLD$$

Where,

STB:isthe**ST**abilityofModel**B**ehavior,

$$STB = \frac{\sum_{j=0}^{M} \frac{dj}{uj}}{\sum_{i=0}^{N} \frac{di}{ui}}$$

DTQ : isthe**D**ata**T**ransmission**Q**uality,

D : isthepowerneededtotransmitthe total**D**ata,

E :refersto**E**nergyneededto sendonebyteofdata.

P :refersto**P**robabilityoferrorinthechannel.

K : isaPacketsizeandisconstant

In order to detecting a malicious node in the network, we takes the example of Black Hole attack. In this example, we defined the node as follows.

S–Source,D –Destination,2-MaliciousNode,1,3,4-NonMaliciousNodes

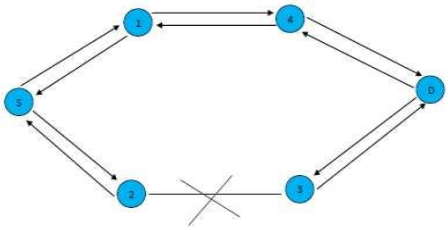

Figure:2. BlackHole attack

Todecide,whethera nodebehavingerraticallyisreallya maliciousnode,wecarryoutthefollowingsteps.

SupposeNode‘S’i.e.thesourcenodeinfigure ‘2’detectsthat theDTQofNode‘2’is belowa thresholdvalue.Consequently node‘S’sendsabroadcast requesttotriggeravote.On receiving thisrequest,thenodesintheMANETcheck their respective tablesfortheDTQvaluesofNode ‘2’, and respondswithapositive oranegative vote.Node‘S’ aggregatesthese votestodecidethe statusofNode‘2’.

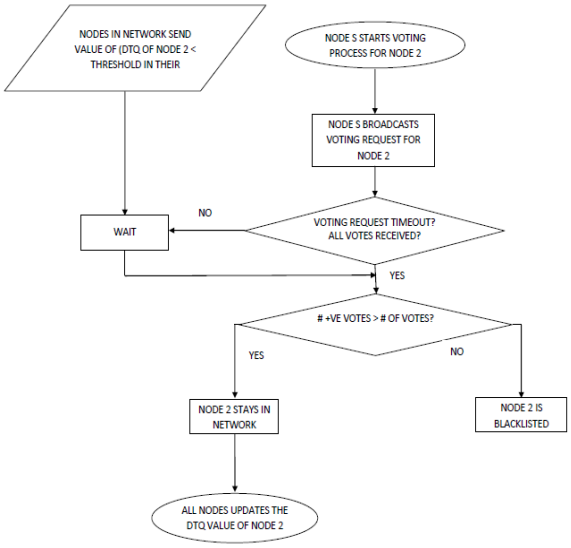

Figure:3.Flowchart fordetectinga MaliciousNode

TheVotingProcessisdetailedasbelow.

TheNode‘S’keepsthecountofnumber ofvotesitreceives fromtheneighboring nodes.Itacceptsonly onevotefrom eachnode.

- Thereisatimelimitsetforreceiving thevotesfromthe neighboring nodes.Onlythevotesreceivedwithinthe stipulatedtimeisaccountedforaggregation.
- All theneighboringnodesthatreceivethe votingrequest attemptstojointhevotingprocess.
- Ifnode‘2’isblacklisted, amessageissenttoallthenodes aboutthisinformation. Allthenodesadd Node‘2’intheir blacklistdetails.
- Ifthenode‘2’isacquittedafterthevoting,all thenodes treat node‘2’asa normalnode.

V. SIMULATION SETUP & 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 Drop and Network Throughput, has been used.

Parameter	Value
Number of Nodes	50
Routing Protocol	AODV
MAC Layer	IEEE 802.11
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	1to 8 Nos.
Packet Sizes	512bytes

a. Malicious Attacks without IDS

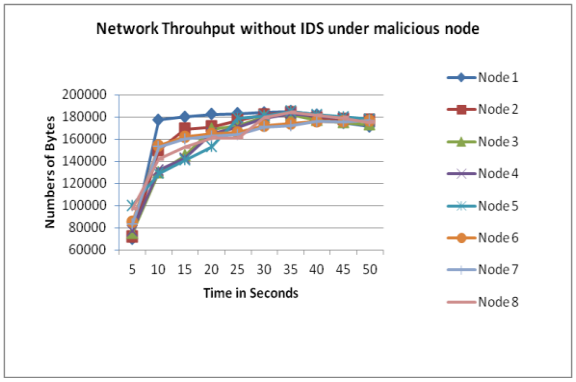

Figure: 4. Throughput without IDS under Malicious Nodes

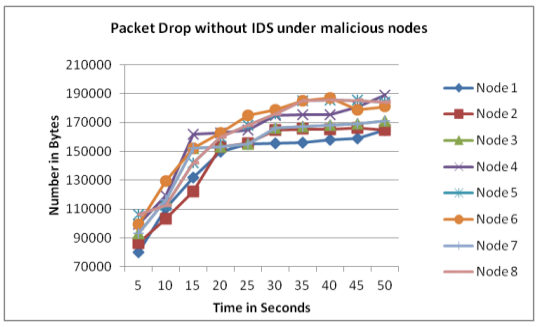

Figure: 5. Packet Drop without IDS under Malicious Nodes

b. Malicious Attacks without IDS

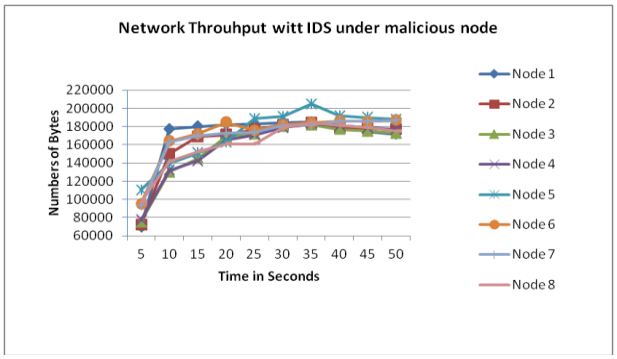

Figure: 6. Throughput with IDS under Malicious Nodes

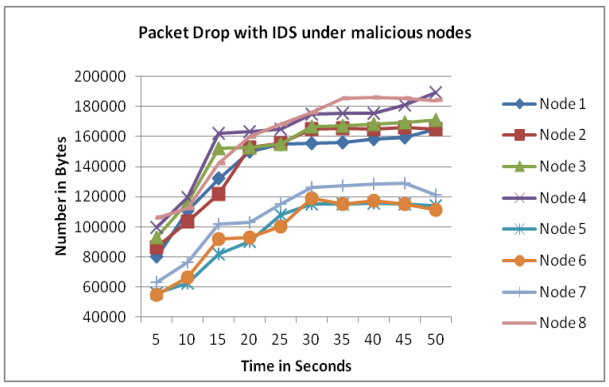

Figure: 7. Packet Drop with IDS under Malicious Nodes

VI. CONCLUSION AND FUTURE WORK

Oncethemalicious nodeisidentified,itisisolatedfromthe systemorisignoredforfuturecommunication,inthenetwork. From thegraphswecanseetheoverallnetwork connectivity and the data loss are heavily affected under these attacks. Further, asthenumber ofblackholeattacks increasesfrom onenodetoeightnodes,thepacketdropalso increases.Withoutanyattack,thepacket dropisminimuminthesimulation. Thenumberofpacketlossgetsreducedwiththe introduction ofIDSintheAODVprotocol.Afterimplementing IDS,with5,6or7numberofBlackholenodes (malicious node),thethroughput ofthesystem improves. ThereforeitcanbeconcludedthatourdevelopedIDSprovid es improvement insystemperformanceforaoptimalnumberof maliciousnodesinthe network.Wecancarryoutsimilarsimulationswithdifferent routingprotocols.

REFERENCES

[1] Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[2] 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.

[3] Vijay Kumar, Rakesh Shrama, Ashwani Kush, “ Effect of Malicious Node on AODV in Mobile Ad Hoc Networks”, International Journal of Computer Science & Management Research, Vol. 1 ,pp. 395-398,October 2012.

[4] Pradip M. Jawandhiya,Mangesh M. Ghonge,Dr. M.S.Ali,Prof. J.S. Deshpande, “A Survey of Mobile Ad Hoc Network Attacks ”, International Journal of Engineering Science and Technology,Vol. 2(9), 2010, 4063-4071

[5] S.Buchegger,C.Tissieres,andJ.Y.LeBoudec.“Atestbedformisbeh aviordetectioninmobilead- hoc networks”.TechnicalReportIC/2003/72,EPFL-DI-ICA,November2003.Available on:citeseer.ist.psu.edu/645200.html.

[6] S.BansalandM.Baker.“Observation-Based Cooperation Enforcement inAdhocNetworks”, July 2003.Availableon: http://arxiv.org/pdf/cs.NI/0307012.

[7] P. Michiardi andR. Molva. Core: “A Collaborative Reputation Mechanism to Enforce Node Cooperation inMobile Ad Hoc Networks”, InProceedings ofthe 6thIFIP .Communications andMultimediaSecurityConference,pages107121,Portorosz,Slovenia,September2002.

[8] KhairulAzmi,AbuBakarandJamesIrvine."AScheme forDetecting SelfishNodesinMANET usingOMNET++", 2010SixthInternational Conference onWirelessandMobileCommunications, pp411-414,2010.

[9] Marti,S., Giuli,T. J.,Lai,K.,&Baker,M.(2000),“Mitigatingroutingmisbehaviorin mobilead-hoc networks”, Proceedingsofthe6thInternational Conference onMobileComputing andNetworking (MobiCom),ISBN1-58113-197-6,pp.255-265.

[10] P Das S. Perkins C.E., Belding-Royer E.M. Ad-hoc on-demand distance vector (aodv) routing. RFC 3561, IETF Network Working Group, 2003.

[11] Pucha H. Hu Y.C. Koutsonikolas D., Das S.M. On optimal ttl sequence-based route discovery in manets. volume vol.9, p.923, 2005.

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

[13] Datuk Prof Ir Ishak Ismail & Mohd Hairil Fitri Ja’afar,"Mobile Ad Hoc Network Overview", Asia-Pacific Conference On Applied Electromagnetics Proceedings, 2007.

[14] Bhupendra B Patel, “Study of Malicious Node in AODV Routing Protocols”, International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 5, May 2013.