Analytical Termination of Malicious nodes (ATOM): An Intrusion Detection System for Detecting Black Hole attack in Mobile Ad hoc Networks

S. Sivanesh
Anna University Chennai - Regional Office Tiruchirappalli
V R Sarma Dhulipala (dvrsarma@gmail.com)
Anna University , BIT Campus

Research Article

Keywords: MANET, AODV, Black hole, Intrusion detection system, ATOM

Posted Date: March 23rd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-178522/v1

Version of Record: A version of this preprint was published at Wireless Personal Communications on November 30th, 2021. See the published version at https://doi.org/10.1007/s11277-021-09418-8.

Abstract

The decentralized administration and the lack of an appropriate infrastructure causes the MANET prone to attacks. The attackers play on the vulnerable characteristics of the MANET and its underlying routing protocols such as AODV, DSR etc to bring about a disruption in the data forwarding operation. Hence, the routing protocols need mechanisms to confront and tackle the attacks by the intruders. This research introduces the novel Host-based Intrusion Detection System (HIDS) known as Analytical Termination of Malicious nodes (ATOM) that systematically detects one of the most significant black hole attacks that affects the performance of AODV routing protocol. ATOM IDS performs detection by computing the RREP count (Route Reply) and the packet drop value for each individual node. This system has been simulated over the AODV routing protocol merged with the black hole nodes and the resultant simulation scenario in NS2 has been generated. The trace obtained shows a colossal increase in the packet delivery ratio (pdr) and throughput. The results prove the efficacy of the proposed system.

I. Introduction

Recent advancements in wireless communication has proportionally amplified the usage of portable devices such as mobile phones, laptops, tabs etc. In MANETS, the wireless communication takes place between random mobile nodes that cooperatively act as routers to perform the data forwarding operation[1]. Nodes in MANET are self-configurable and are deployed randomly to establish communication under intense conditions such as disaster relief operation, military based operation, emergency situations etc. as they are open to swift adaptations on demand. The entire MANET communication is instituted upon on demand routing protocols such as AODV, DSR, DSDV etc. MANETS are devoid of a centralized administration and the infrastructure-less nature of the network is inclined to several attacks by the intruders. The lack of security mechanism in the AODV protocol paves the way for the intruders to directly aim at exploiting the vulnerabilities of the routing protocol. The attacks on network layer's routing protocol [2-4] compromises the nodes and its ability to deliver the packets to the intended destination. In AODV protocol [5], the route discovery procedure is initiated when the source node broadcasts a route request (RREQ) to the neighboring nodes within its communication range in search of a destination. The source waits for a specific time period for the Route reply (RREP) by the intermediate nodes and resends the RREQ once the former RREQ gets timed out. The RREP is not only sent by the nodes that legitimately recognize the destination mentioned in the RREQ packet but also by the malicious nodes that intentionally send a false RREP even though it is unaware of the location of destination. In accordance with the AODV protocol, the RREP packet by the node with the highest sequence number possesses the best fresh route to the designated destination.

The Intrusive black hole attack [15] is a perilous attack caused by the malicious nodes that deteriorate the entire network by broadcasting a fake fresh route to the destination by sending a RREP with a massively high destination sequence number and therefore draws the data packets towards itself resulting in the disruption of the services like dropping those data packets instead of forwarding them. The AODV protocol is blindsided from distinguishing between the authentic and malicious nodes as they cannot

comprehend the legitimacy of the RREP. The intermediate malicious nodes that intentionally fake the RREP are also assumed as a trusted node by the AODV protocol which directly leads to a decrease in the packet delivery ratio. To tackle the vulnerability of the AODV protocol, copious intrusion detection systems were developed to detect, prevent and to punish the misbehaving nodes. The immediate reaction of any decent intrusion detection system is to occlude the detected malicious node from the ongoing communication. In the Host based Intrusion Detection System (HIDS), every node in the network acts as an IDS by detecting the data traffic flowing through it. Watchdog is the most prominent intrusion detection system that runs over the DSR protocol. It is a monitoring mechanism that looks over its neighboring nodes and detects any deviation in the behavior of those nodes by overhearing the packet forwarding process. However, the watchdog IDS is compatible only with the DSR protocol and isn't feasible for AODV routing protocol.

In this paper, we have proposed a host based intrusion detection algorithm ATOM (Analytical Termination of Malicious nodes) that is solely designed for AODV routing protocol so as to champion the adverse consequences of the intruding malicious nodes that attack the susceptible features of MANET. ATOM runs on every node and monitors the node's route reply count and the subsequent packet drop values. ATOM increments the RREP count for every node in its previous hop node's routing table and monitors the corresponding packet delivery status for that node. If a node exhibits abnormal behavior during detection, then the node is a malicious imposter posing as a legitimate node in the route discovery process.

The malicious node is then isolated and discarded from participating in the routing procedure and no further RREPs from that node will be acknowledged by its previous hop nodes. Thus the security feature of the AODV protocol is strengthened by reducing the packet loss and eliminating the intruders in the network. Hence, our proposed system leads to an increase in the packet delivery ratio and throughput.

The rest of the paper has been organized as follows. Section II, we have addressed related works, Section III introduces system ATOM-An IDS for MANET and Section IV- we describe the simulation environment and result analysis final Section concludes the research paper.

Ii. Related Works

Marti et al. [6] proposed an IDS watchdog and path rater scheme for securing MANET from packet dropping attack. This scheme looks over its next hop neighbor node's transmission, and increments the suspicious count when a monitored node fails to forward its received packet intended for other destination. System will alarm if the suspicious value exceeds the threshold limit. Path rater avoids routes that contain malicious nodes to perform secure routing operations.

Sonja Buchegger et al. [7] proposed a routing protocol CONFIDANT with four modules: monitoring system, reputation system, trust manager and path manager. Each node monitors its neighbor nodes for updating the reputation value of overhearing nodes and performs the routing operation accordingly.

Hassan et al. [8] proposed specification-based intrusion detection for AODV to regulate the routing operations. Using a clustered network monitoring selection algorithm a network monitoring node (NM) is elected to monitor the exchange of RREQ and RREP messages. The NM node will ensure the integrity of Routing messages to perform the routing operations.

Shakshuki et al. [9] proposed an acknowledgment-based ID for MANET- Enhanced Adaptive Acknowledgment (EAACK). DSA and RSA algorithms have been used for authenticating the exchange of acknowledgement packets to overcome the several network layer attacks.

Ming-Yang Su [10] proposed IDS for mitigating black hole in MANET by evolving the suspicious value of a node. The abnormal difference between the RREQ and the RREP of a node will be considered for the evaluation of this suspicious value. If the suspicious value reaches the threshold value, nearby IDS will broadcast the block message to every other node to block and isolate that node from the network.

Payal N. Raj et al. [11] Proposed a protocol DPRAODV which defends against black hole. If the RREP's sequence number of a reply packet is greater than that of the threshold value computed by Detection, Prevention and Reactive AODV (DPRAODV) then that node will be suspected as malicious

A. R. Rajeswar et al. [12] Proposed GNB-AODV for detecting black hole node with fixed deployed guard nodes. Guard node maintains Packet Monitoring Table (PM) and Malicious Node Table (MN) for updating the node's behavior during the route discovery procedure of AODV. All the RREQ of overhearing nodes will be logged in the PM table and the trust value will be evaluated in the MN table. According to their proposed method a node which didn't broadcasted any RREQ but forwards RREP to the specific route will be treated as an anomaly. Further the trust value of that node will be decremented. If the trust value decreases the predetermined threshold value, the guard node will alarm his overhearing nodes to isolate that node form network. This information will be updated in Black listed table owned by a normal node.

Sivanesh.S et al. [13] proposed an IDS Accurate and cognitive intrusion detection system (ACID) for detecting black hole attack. Parameters like destination sequence number and route reply count are considered for the evaluation of Black hole node. ACID detects the highly fabricated sequence number of AODV messages and compares them with the route reply count. If a node's RREP count and its difference of DSN exceed the threshold limit, ACID confirms that node as a malicious black hole and discards RREP.

Iii. Proposed System

The AODV routing protocol initiates the route discovery procedure on demand in search for a destination node with the aid of three control packets namely RREQ, RREP and RERR. In MANET, every node maintains a routing table which constantly updates the information regarding the destination sequence number, hop count, network address etc.

The source node broadcasts a RREQ to its nearby neighbor nodes awaiting a RREP in return to its request. The intermediate nodes that receive the RREQ examine its own routing table regarding the

sequence number information related to the destination. If the sequence number in the routing table for the corresponding destination in the incoming RREQ packet is higher than the one specified by the source node, then a RREP is unicast back to the originator of the Route Request. The malicious node poses as an intermediate node and allures the data packet to be forwarded through the path in which it is present by forging the RREP packet providing it with a high sequence number. Several Intrusion Detection Systems were developed in the past to reduce and eliminate the negative impact of malicious nodes on the MANET.

The ATOM is a host-based IDS that accurately discovers those malicious nodes with the aid of evaluation metrics such as Route Reply Count (RREP COUNT) and Packet Drop (PD).The malicious nodes sends a RREP whenever a RREQ is sent to it irrespective of their knowledge of location concerning the destination node. Hence, the route reply count of a malicious node will always be high when compared with an authentic intermediate node. Taking advantage of this factor, we craft an additional RREP COUNT field in the routing table of every node to reckon the total number of RREPs sent by that node. The node increments the RREP count in the routing table whenever it responds to a RREQ from the source node.

A threshold value is prefixed and if the RREP count for each node after increment exceeds the threshold limit, then the particular node's behavior is manifested as suspicious. The RREP count of authentic nodes that actively take part in the routing operations is also incremented in the routing table and hinted as suspicious upon surpassing the threshold limit.

In order to avoid an increase in the false positive rate and to confirm our uncertainty on the actively responding legitimate nodes marked as suspicious through the increment of RREP COUNT, the corresponding packet drop value for all the nodes in the routing process has been considered. The ATOM algorithm overhears the recipient status of the packets sent to its neighboring nodes and the packet drop value and calculates the ratio between the forwarded and dropped packets by that node. If the ratio between the total number of packets forwarded by the node and the total number of packets sent to that node is lesser than the ratio of the total number of packets dropped to the summation of packets dropped and forwarded, then the node has intentionally dropped packets in addition to the loss of packets due to collision.

$$\frac{Packets_{forwarded}}{Packets_{forwarded} + Packets_{dropped}} < \frac{Packets_{dropped}}{Packets_{forwarded} + Packets_{dropped}}$$

The nodes that have intentionally dropped packets and the nodes that were deemed as suspicious through the RREP COUNT procedure are cross correlated with one another by the ATOM IDS to check for malicious behavior. If the RREP COUNT has surpassed the threshold limit for a node and its corresponding packet drop value is significantly high, then the node is fixated as malicious node.

The packet drop value for the legitimate nodes actively involving themselves in the route discovery procedure will be low in comparison with the intentional malicious packet droppers and hence the false positive rate in our proposed system can be overcome with the aid of packet drop parameter. Further, the nodes that are condemned as malicious are excluded from associating themselves with any route discovery related operation. By doing so, the packet delivery ratio and throughput of the AODV is vastly improved with an immense decrease in the packet loss count of each node. Fig.1 (a) shows the block diagram of the proposed system ATOM followed by pseudo code

Pseudo Code- ATOM

Initialize route discovery

Send route request

IF(fresh route)

Send routereply

//creating new entry in Sendreply

Declare new entry as rt

Initialize rt in rt_entry

IF(rt)

Assign rt as rtable.lb_first

//Initialize rreply_cnt

Set rreply_cnt to zero

Sendreply(Packet)

Increment rreply_cnt

If (rreply_cnt > threshold)

Declare susp_value

Set susp_value to true

//Comparing with Packets_dropped

IF(Packets are not_forwarded)

Increment dropped_packets

IF(dropped_packets greater than max_packets_lost)

Set max_packets_lost = dropped_packets

Declare boolean z

Initialize z as false

IF(forwarded ratio is lesser than dropped ratio)

Set z as true

```
//Passing arguments to aodv.cc
IF(better route)
 Update route entry
IF((susp_value is true) and (z  is true)) //it is a intruder
//drop the route reply
DROP _ROUTE_REPLY
Else
// it is a legitimate node
Forward reply
Update route table
```

Iv. Performance Evaluation

The analytical detection and the performance of ATOM have been evaluated in the NS2 [14] environment and the simulation specification are listed inTable 1

TABLE 1. Simulation Scenario

CHANNEL TYPE	WIRELESS CHANNEL
MAX.PACKET IN IF- QUEUE	68
MOBILE NODE DENSITY	50
PROTOCOL	AODV
X-DIMENSION	1211
Y-DIMENSION	596
SIMULATION PERIOD	10 minutes
NO.OF MALICIOUS NODES (%)	5 ,10,15&20
NO. OFCOMMUNICATION	12
PACKET SIZE	512 bytes

The simulation scenario of MANET comprised of 50 mobile nodes and simulated 5 diverse scenarios in NS2 where each scenario dealt with a varied number of malicious nodes such as 5, 10, 15 and 20. The evaluation metrics of ATOM such as PDR, packet loss, throughput &routing overhead are measured up with the AODV routing protocol infested with blackhole nodes. A total of 12 communications took place and the time period for the entire communication was set to 20 min. The simulation traces were obtained and the results are depicted in Fig. 2a, (b), (c) and (d).

Fig. 2a, (b), (c) and (d) packet delivery ratio (pdr) of ATOM and AODV with black hole of 5,10,15 & 20 malicious nodes.

Figure 2a, (b), (c) and (d) clearly indicate the obvious fact that the proposed system ATOM has greater pdr when compared with the existing AODV protocol. ATOM with 5 &10malicious nodes deliver the packet 50-60% more efficiently than the existing AODV protocol and a 40-50% increase in the packet delivery ratio when the malicious node density is 15& 20.

Fig. 3a, (b), (c) and (d) Packet loss of ATOM and AODV with black hole of 5, 10, 15 &20 malicious nodes.

Fig. 3a, (b), (c) and (d) depict the obvious fact that the ATOM has a lower packet loss when compared with the existing AODV protocol. The ATOM shows that with 5 &10malicious nodes the packet loss value dropped to 60-70% more than the existing AODV protocol and a 40-50% decrease in the packet loss value when the malicious node density was fixed to 15& 20.

Fig. 4a, (b), (c) and (d) Routing overhead of ATOM and AODV with black hole of 5,10,15 &20 malicious nodes respectively.

Since the ATOM IDS discards the Route Reply (RREP) packet of the malicious nodes, the source node re-initiates the route discovery procedure that consequently leads to an increase in the total number of control packets sent during the communication period. Fig. 4a, (b), (c) and (d) portrays an 10-20% increase in the routing overhead with 5 & 10 malicious nodes and an 30-40% increase in the routing overhead when the malicious node concentrations are fixed to 15 & 20.

Fig. 5a, (b), (c) and (d) Throughput of ATOM and AODV with black hole with 5, 10, 15 &20 malicious nodes respectively.

Fig. 5a, (b), (c) and (d) shows that the proposed system ATOM has a greater throughput when compared with the existing AODV protocol. The throughput of ATOM with 5 &10 malicious nodes is 50-60% more efficient than the existing AODV protocol and a visible 40-50% increase in the throughput of ATOM when the malicious node density is 15& 20.

V. Conclusion

In this paper, we have developed an IDS Analytical Termination of Malicious nodes (ATOM) for Detecting Black Hole attack in Mobile Ad hoc Networks. Based on the analysis of various simulation scenarios, it is evident that results validate the efficiency of the proposed system ATOM on detecting black hole nodes with increased PDR and throughput.

Declarations

COMPLIANCE WITH ETHICAL STANDARDS

ETHICAL APPROVAL

This article does not contain any studies with human participants performed by any of the authors. (Or) This article does not contain any studies with animals performed by any of the authors. (Or) This article does not contain any studies with human participants or animals performed by any of the authors.

CONFLICT OF INTEREST

There is no conflict of interest exists between the authors or financial or personal relationship with a third party whose interests could be positively or negatively influenced by the article's content.

INFORMED CONSENT

This article does not contain any human participants in the study

References

1. IETF Mobile Ad-Hoc Networks Working Group (MANET),IETF website, ietf.org/dyn/wg/charter/manet-charter.html.
2. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE.*, vol. 13, no. 6, pp. 24–30, Nov./Dec. 1999.
3. Nadeem and M.P.Howarth, "A survey of manet intrusion detection & prevention approaches for network layer attacks, "Communications Surveys & Tutorials, IEEE, vol. 15, no. 4, pp. 2027-2045, 2013.
4. Kumar, S. and Dutta, K., 2016. Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges. *Security and Communication Networks*, *9*(14), pp.2484-2556.
5. Ad hoc On-Demand Distance Vector (AODV) - Routing protocol https://tools.ietf.org/html/rfc3561
6. Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", ACM, pp. 255–265,2000.
7. Buchegger, S. and Le Boudec, J.Y., 2002, June. Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*(pp. 226-236). ACM.
8. Hassan, H.M., Mahmoud, M. and El-Kassas, S., 2006, October. Securing the AODV protocol using specification-based intrusion detection. In *Proceedings of the 2nd ACM international workshop on Quality of service & security for wireless and mobile networks*(pp. 33-36). ACM.
9. Shakshuki, E.M., Kang, N. and Sheltami, T.R., 2012. EAACK—a secure intrusion-detection system for MANETs. *IEEE transactions on industrial electronics*, *60*(3), pp.1089-1098
10. Su, M.Y., 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*, *34*(1), pp.107-117.
11. Raj, P.N. and Swadas, P.B., 2009. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. *arXiv preprint arXiv:0909.2371*.
12. Rajeswari, A.R., Kulothungan, K. and Kannan, A., 2016. GNBAODV: guard node based–aodv to mitigate black hole attack in MANET. International Journal of Scientific Research in Science,

Engineering and Technology, 2(6), pp.671-677.

13. Sivanesh, S. and Dhulipala, V.S., 2020. Accurate and cognitive intrusion detection system (ACIDS): a novel black hole detection mechanism in mobile ad hoc networks. Mobile Networks and Applications, pp.1-9.
14. The Network Simulator NS-2 version 2.35 http://www.isi.edu/nsnam/ns/index.html.
15. Sivanesh, S. and Dhulipala, V.S., 2019, May. Comparitive Analysis of Blackhole and Rushing Attack in MANET. In 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW) (pp. 495-499). IEEE.
16. Marathe, N. and Shinde, S.K., 2019. ITCA, an IDS and trust solution collaborated with ACK based approach to mitigate network layer attack on MANET routing. *Wireless Personal Communications*, *107*(1), pp.393-416.

Figures

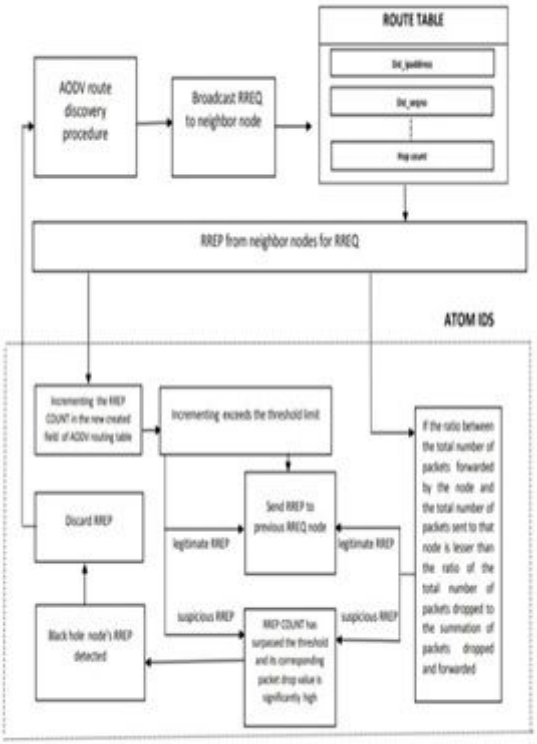

Figure 1

Block diagram of proposed ATOM

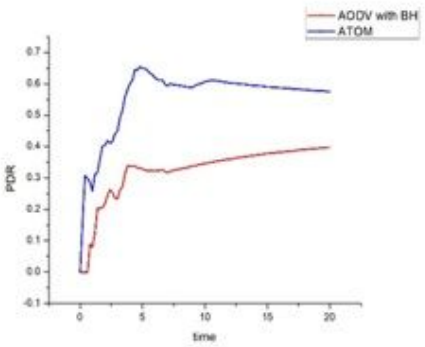

Fig. 2(a).PDR for 5 malicious

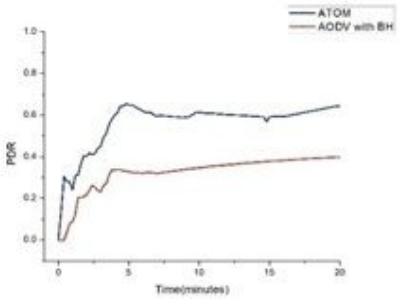

Fig. 2(b). PDR for 10 malicious

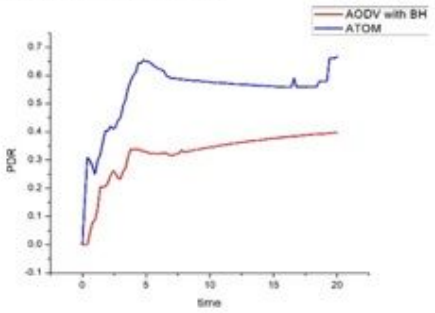

Fig. 2(c). PDR for 15 malicious

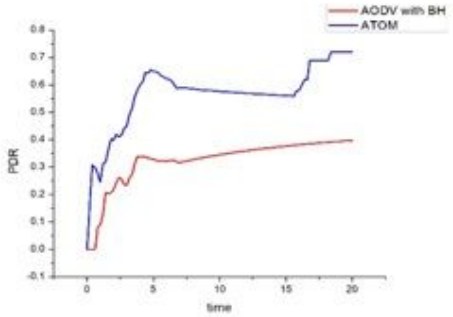

Fig. 2(d). PDR for 20 malicious

Figure 2

(a), (b), (c) and (d) packet delivery ratio (pdr) of ATOM and AODV with black hole of 5,10,15 & 20 malicious nodes.

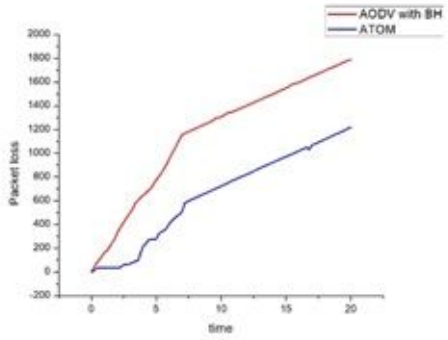

Fig. 3(a).packet loss for 5 malicious

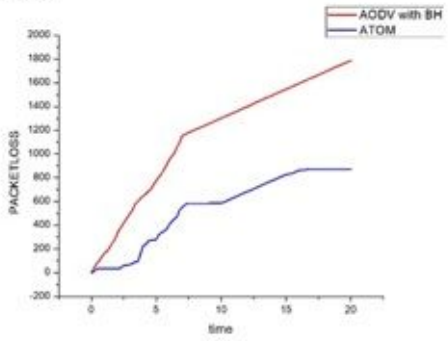

Fig. 3(b).packet loss for 10 malicious

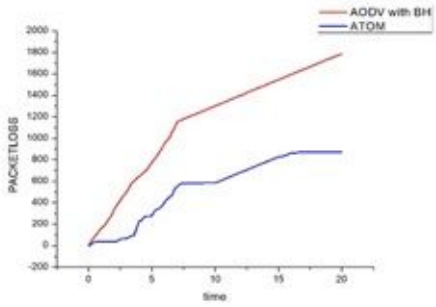

Fig. 3(c).packet loss for 15 malicious

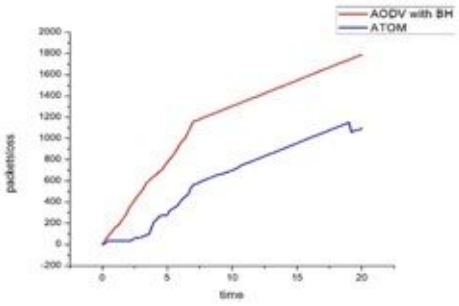

Fig. 3(d).packet loss for 15 malicious

Figure 3

(a), (b), (c) and (d) Packet loss of ATOM and AODV with black hole of 5, 10, 15 &20 malicious nodes.

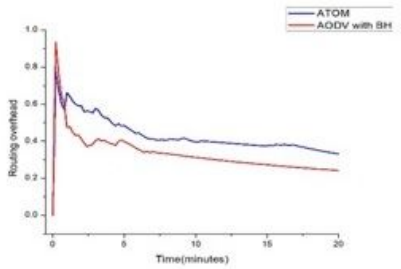

Fig. 4(a).Routing overhead for 5 malicious

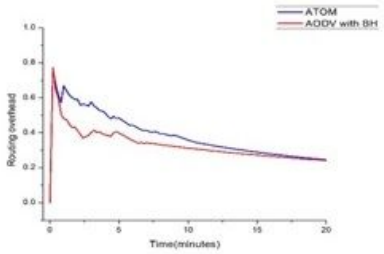

Fig. 4(b).Routing overhead for 10 malicious

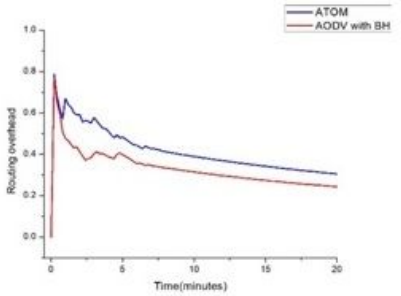

Fig. 4(c).Routing overhead for 15 malicious

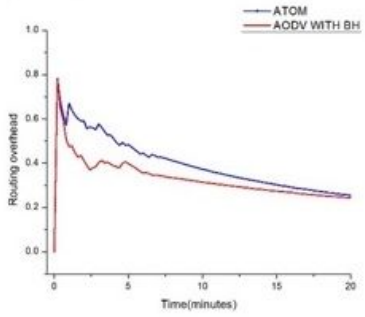

Fig. 4(d).Routing overhead for 20 malicious

Figure 4

(a), (b), (c) and (d) Routing overhead of ATOM and AODV with black hole of 5,10,15 &20 malicious nodes respectively.

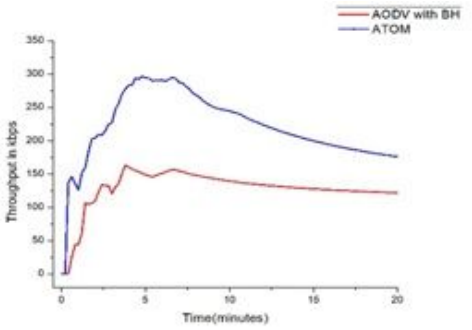

Fig. 5(a).Throughput for 5 malicious

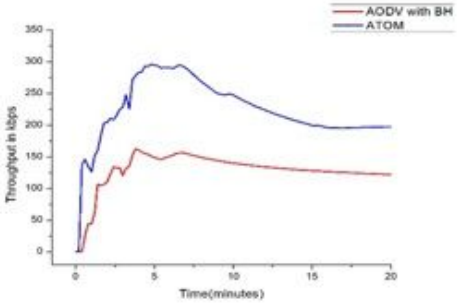

Fig. 5(b).Throughput for 10 malicious

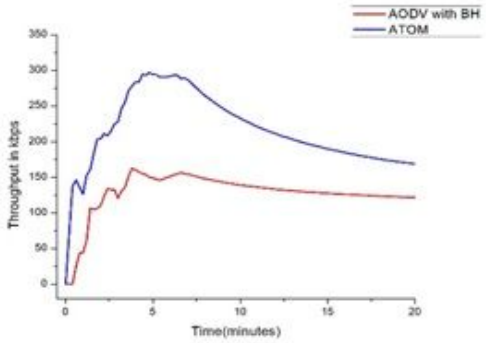

Fig. 5(c).Throughput for 15 malicious

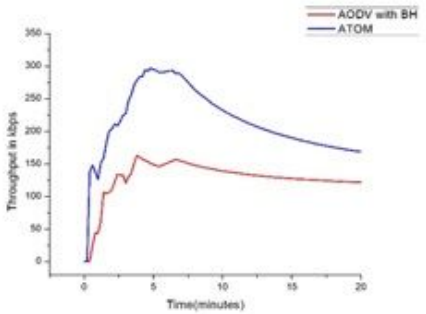

Fig. 5(d).Throughput for 20 malicious

Figure 5

(a), (b), (c) and (d) Throughput of ATOM and AODV with black hole with 5, 10, 15 &20 malicious nodes respectively.