Secured AODV to Prevent Single and Collaborative Black Hole Attack in MANETs

Charu Wahi

Abstract: ***This paper addresses one of the most important security attacks against routing in Mobile Ad Hoc Networks – Black hole attack. We propose an algorithm called Secured AODV (SAODV) to reduce the susceptibility of AODV routing protocol against Black hole attack. The proposed algorithm combats the effect of both single and collaborative Black hole attack. Essentially it requires the intermediate node to validate the Sequence Numbers and Speed of node (which replies with a route to the destination) based on well-defined thresholds prior to instantiating a communication with destination to send data packets; without imposing any additional overhead on source and destination nodes.***

A very small number of solutions exist that can collectively prevent both single and collaborative black hole attacks. Moreover, those who do, have high amount of overhead and delay. Simulation using NS-2 shows that SAODV provides better security against single and collaborative blackhole attacks and also better performance in terms of Packet delivery ratio and Throughput against original AODV in presence of Blackhole nodes. In comparison to AODV, there is an improvement in PDR by 60-80% and throughput increases by 70-80% when malicious nodes are present in the network; with a marginal increase in delay and overhead.

Keywords: MANET, AODV, SAODV, Black-Hole, Single, Collaborative

I. INTRODUCTION

In the current age, the study of Mobile Ad-hoc NETworks (MANETs) has secured researchers' attention due to the recognition of the emerging computing paradigm [1]. A MANET is a self-configuring network of wireless mobile nodes that create a network with dynamically changing topology. They are characterized by self-organization, dynamic topology, limited resources, self-configuration and lack of infrastructure. These features make MANETs best suitable for applications like disaster recovery operations, emergency search and rescue, battlefields and smart buildings or class rooms.

The dynamic topology, wireless nature, lack of a fixed infrastructure and centralized control, make MANETs vulnerable to the security intrusions. In this article, we propose to strengthen the prevailing routing protocols to facilitate secure routing for MANETs. These routing mechanisms are particularly susceptible in MANETs because of the dependence of these algorithms on nodes cooperation to establish communication.

Revised Manuscript Received on May 22, 2019.

Charu Wahi, Birla Institute of Technology, Mesra, Noida Campus

One of the principal routing protocols used in MANETs is Ad-hoc On-demand Distance Vector (AODV) [2]. AODV is a reactive routing protocol that has been designed without security considerations. The network layer in MANETs is vulnerable to numerous attacks like Denial-of-service attacks namely Sinkhole, Wormhole, Blackhole, and Grayhole attacks**,** information disclosure attack, Sybil attacks, routing attacks viz. packet replication, route cache poisoning and rushing attacks. Amongst these, we focus on examining and enhancing the security of AODV routing protocol against Blackhole attacks. The simulation results and investigation shown in section 5 testifies that the proposed solution effectively improves security of AODV, in preventing both single and collaborative Blackhole attacks in MANETs with insignificant performance penalty.

This paper proceeds as follows: Section 2 provides the problem statement by giving an insight on AODV routing protocol and then Blackhole attack. Next in section 3, we have discussed the work of researchers to mitigate the effect of Black-Hole attack against AODV. In section 4, we discuss the proposed algorithm SAODV. And section 5 describes the simulation setup, its results and analysis. Lastly, section 6 concludes the paper and discusses the future research directions.

II. PROBLEM STATEMENT

A. Overview of AODV

AODV is a routing mechanism that implements a purely reactive approach; it establishes a route whenever needed towards the beginning of a conversation and utilizes till it breaks. It employs Route REQuest (RREQ) and Route REPly (RREP) packets during route discovery stage and Route ERRor (RERR) packet in route maintenance stage. More about these messages can be seen in [2].

Being a reactive strategy, AODV only has to retain the routing information regarding the active routes. Every node in the network stores this data in the routing tables. Each of the mobile node retains a next hop routing table, which is a collection of routes to distinct nodes within the network. Information in the table perishes if it has not been utilized for a pre-designated expiry time.

"One unique feature of AODV is its use of a sequence number, a monotonically increasing number maintained by each originating node, for each route entry". Every entry must comprise the most recent information related to the sequence

number for the destination node, for which the route reply is maintained. This sequence number is called "destination sequence number". It is updated each time a node receives fresh information regarding the sequence number from RREQ, RREP or RERR messages. "Using destination sequence numbers ensures loop freedom and is simple to program" [2].
In AODV, as soon as a device needs to initiate communication with any other device, it initiates a route discovery operation if no route is available in the routing table. The source node broadcasts a RREQ packet which includes Destination Sequence Number, in the route discovery process (fig. 1). Once an intermediate or destination device, which has a route to the destination receives the RREQ packet, it examines the destination sequence number it presently recognizes and the one indicated in the packet. In order to maintain freshness in the network, a RREP frame is created and forwarded back to the source node only if the destination sequence number is equal to or greater than the one specified in RREQ.

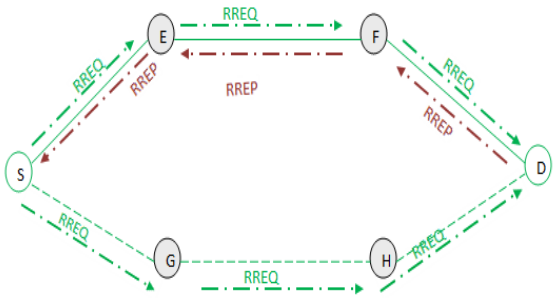


Figure 1: Route Discovery Process in AODV

B. Black-Hole attack
Blackhole attack belongs to the category of the Denial-of-service (DoS) attacks in ad hoc networks that disrupts the working of network layer. "In this attack, a malicious node sends a false RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an intermediate node to the actual destination node" [1]. Thereon, source will transmit all its data messages towards the illegitimate node. The malicious node ultimately will never forward the data packets to the intended destination. Consequently, source and destination will never be able to establish a communication together.
The black hole node is a malicious node that joins the network with the intention of dropping the transmitted data packets instead of delivering them to the desired destination [4]. An example is shown in fig. 2. In AODV, upon receiving a number of RREP, a source node selects the one with greatest Destination sequence number to construct a route. To succeed, a blackhole node must generate its RREP with Destination sequence greater than that of the destination node.

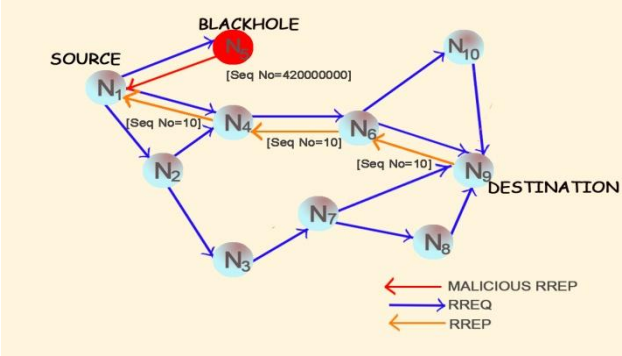


Figure 2: Single Black Hole Attack

It is quite possible that some malicious nodes will collaborate together in order to capture the routing information and moreover, hide from the existing routing mechanism. When numerous black hole nodes work in collaboration with the intention of disrupting the normal flow of communication, is known as collaborative black hole attack, node *N2* sends the RREP and identifies the route through node *N3* (fig. 3).

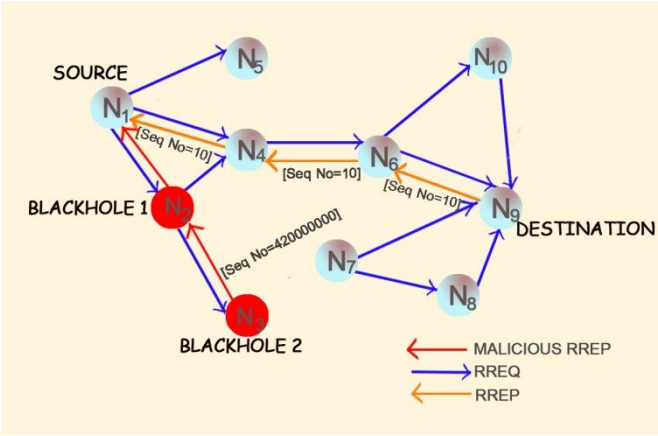


Figure 3: Collaborative Black Hole Attack

III. RELATED WORK

Research to mitigate the effect of blackhole attack against AODV in MANETs is an evolving process. Many researchers have proposed solutions to reduce the effect, here is an overview:
In [5], Deng *et al*. proposed a solution for single black holes. According to their solution, when any intermediate node sends RREP it should have information about the next hop to destination. The source device doesn't transmit data packets to an intermediate node instantly. It rather waits for the RREPs and then transmit a further request (FREQ) packet to next hop of replied node and enquires regarding the replied node and route to the destination. The next hop node sends FurtherReply packet to the source. If it does not have a route, then the source will transmit an alarm packet to alarm other nodes. However, this solution is unable to avert cooperative black hole attacks. For instance, if the next hop also collaborates with the replied device, the reply for the FREQ will be simply "yes" for both questions. At that time, the source will trust next hop and send data through the replied

node which is a black hole node.

In [6], the authors proposed an approach that involves a source node to wait until a RREP packet arrives from more than two nodes. After receiving multiple RREPs, the requesting node examines if there is a shared hop or not. If there is, the source concludes that the route is safe. The main limitation of this approach is that it takes more time, because it is required to wait for several RREPs to arrive.

The authors in [7] talk about an approach in which the source node waits for the responses from other neighboring nodes for a pre-established time. After the timeout, it first inspects for a repeated next-hop node in the Collect Route Reply Table (CRRT) table. If any such node is present in the reply routes, it presumes the routes are safe or the possibility of malicious paths is limited. The drawback of the approach is that it adds a delay and there is an additional overhead involved in the process of finding repeated next hop.

Ramaswamy *et al.* discussed a technique for recognizing multiple black hole nodes [8]. They were the first to propose a solution for cooperative black hole attacks. They revised the AODV protocol to some extent via establishing a Data Routing Information (DRI) table and a cross checking mechanism. This method uses the reliable nodes to transfer the packets. Nevertheless, they only considered those multiple black hole nodes, without any collaboration amongst them.

In [9], authors discuss a protocol SRD-AODV that provides secure route discovery to prevent black hole attacks. The solution entails the source and destination nodes to verify the sequence numbers in the RREQ and RREP packets, based on established thresholds before initiating data communication with the destination. The limitation of this solution is that it does not address collaborative black hole attacks.

Latha Tamilselvan and Dr. V Sankaranarayanan proposed an approach which talks about the cooperative behavior of two black hole nodes functioning together [10]. Every node maintains a fidelity table to record the fidelity values of the participating nodes. This value is incremented or decremented proportional to their behavior. The approach works as follows: a source node sends a RREQ and waits for a pre-established amount of time to gather the RREPs. Once the routes are collected, the source examines the fidelity values of both the replying node and its next hop in each received route. The source node chooses the route with the highest fidelity value and sends its data via that route. If there is more than one route with the same fidelity value, the source chooses the one with least number of hops. Once the destination node receives the data it sends an acknowledgement to the source informing it that it has successfully received the data. On receipt of acknowledgement, the source increments the fidelity values of the replying node and its next hop and decrement them if the acknowledgement is not received. This updated fidelity values are exchanged over the network. When the fidelity value of the replying node drops to zero, both of the node and its next hop are considered as a cooperative team of black hole nodes and eliminated from the network.

In [11], authors provide solution for both single and collaborative black hole nodes, by diverting the traffic from the black hole. The proposed solution GAODV is utilizes the concept of gratuitous RREP packet sent to the destination node. They added few packets: *CONFIRM, CHCKNFRM and REPLYCONFIRM* and tables called *Confirm, ReplyConfirm, BlackHole* and *CollaborativeBlackHole*. However, the protocol suffered from a huge increase in delay to achieve security.

IV. SAODV

A. Terminology

S : Source Node
D : Destination Node
Y : Intermediate node that replies with RREP
X : Node preceding to Y
Z : Node few hops (at the max 2) away from Y enroute to D
Dest_Seq : Destination Sequence Number
Dest_Seq_TH : Destination Sequence Number Threshold
Speed_TH : Speed Threshold
MHELLO : Modified HELLO packet

B. The Proposed Solution

We propose a solution that is an enhancement of the AODV routing protocol and designed to reduce the effect of single and collaborative black hole attacks against the performance of AODV in MANETs. The proposed solution SAODV does not alter the default operations of either the source nodes or destination nodes. The method followed basically modifies the working of the intermediate nodes only, using additional variables to define the threshold of sequence numbers and speed of node. Apart from this, we also added a Modified HELLO (MHELLO) packet which is similar to HELLO packet used in AODV, except with a difference in the value of hopcount.

The working of SAODV relies on a node preceding to the intermediate node that is sending RREP to establish secure connection between S and D. It does not alter the working of the original AODV protocol if S receives RREP from D, which is considered to be reliable.

In [7], the maximum value for the sequence numbers, based on signed 32-bit arithmetic will be 4294967295 and when incremented will have a value of zero. This property of AODV when exploited by malicious nodes deteriorates its performance. Therefore, the intermediate node X (preceding to intermediate node Y who is generating RREP) must resolve which of the messages is a genuine RREP and which one is a fake message generated from the black hole node. To ensure this, SAODV requires the node X to use the defined threshold values of

sequence numbers and node speed. If the Dest_Seq in the RREP message is greater than the Dest_Seq_TH, the intermediate node X considers this message to be a fake message generated by a black hole node and does not forward it to S. Otherwise, it is an authentic message received from any intermediate node Y and hence, X forwards it to S.

The algorithm also incorporates the fact that a malicious node will have tendency to move abruptly and fastly in the network to disrupt its working. Therefore, to verify the authenticity of RREPs received SAODV also checks whether the node speed is greater than the Speed_TH. If true, algorithm proceeds to check collaborative attack.

However, this enhancement will only be effective if malicious node is not working in a group. So, to mitigate the collaborative black hole attack, we add the following process: node X will send a MHELLO packet to a node Z which is few hop counts away from Y. If X successfully receives acknowledgement from Z, it considers all nodes as genuine nodes and forwards RREP to S and hence secure route is established between S and D. in case of no receipt of acknowledgement, X sends an alert signal to S indicating that node Y and Z are malicious nodes. It should be noted that maximum value of hopcount in MHELLO is limited to 3.

C. *Algorithm*

The mechanism above provides efficient performance for detecting and preventing single and collaborative black hole attacks in MANETs. Refer fig. 4 for the algorithm of SAODV.

V. SIMULATION RESULTS AND ANALYSIS

A. *Simulation Environment*

We employ Network Simulator (NS2) to evaluate the performance of SAODV under different conditions [12]. "NS2 is an event-driven simulator tool that is specifically designed to study the dynamic nature of wireless communication networks" [9]. The same connection pattern has been used in all experiments to ensure uniformity and consistency.

The experiment involves creation of ad-hoc networks of 10, 20, 30, 40 and 50 nodes, moving at a speed of 5 m/s in a terrain area of 1000x1000. Each experiment lasts for 300 seconds of simulation time. Table 4.1 lists the fixed simulation parameters. It simulates a network of randomly moving nodes communicating with each other with Constant Bit Rate (CBR), where some nodes behave maliciously.

Table 4.1: Fixed simulation parameters

Parameter	Value
Simulator	NS-2 (2.35)
Area size	1000x1000
Simulation Time	300s
Routing protocol	AODV, SAODV
Traffic model	CBR
Mobility model	Random way point
No. of malicious node	1-3

Table 4.2 shows the variable parameters for simulating SAODV in the two experiments to study the impact of mobility and scalability. These parameters are (i) the number of nodes in the MANET and (ii) The distribution of nodes' speed. Experiment 1 is performed by varying number of nodes from 10 to 50 while keeping the node speed constant. Experiment 2 varies the node speed and maintains constant number of nodes and malicious nodes.

Table 4.2: Variable simulation parameters

Experiment no.	Malicious nodes	Max. speed(m/s)	Number of nodes
1	1, 2	50	**10-50**
2	3	**5-25**	30

B. *Scenario*

Various scenarios have been designed in NS-2 to assess the performance of SAODV in presence of Black Hole attacks by varying network size, number of malicious nodes and node speeds. A screenshot of a network of 30 nodes with 3 blackhole nodes is shown in fig. 5.

Figure 5: Screenshot of MANET with 30 nodes and 3 blackhole nodes

C. *Metrics used for Simulation*

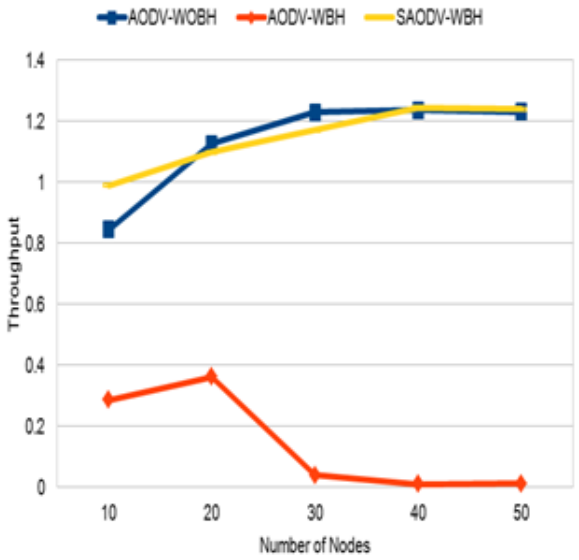
We use the following metrics to evaluate the performance of the routing protocols:

- **Throughput**: the number of data packets successfully delivered per unit time through a network [3].
- **Packet delivery ratio (PDR)**: the ratio of packets received by the destination node to the total number of packets sent by the source node.
- **Average end-to-end delay**: the average time taken for a data packet to be transmitted across the network from source to destination [3].
- **Normalized routing load (NRL)**: the total number of control packets transmitted for routing per data packet sent by the source node. This metric is also highly correlated with the number of route changes occurred in simulation.

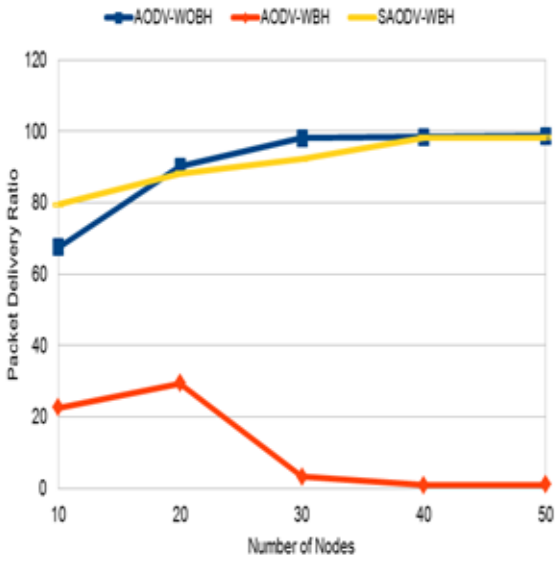
D. *Graphs and analysis*

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

To prove the efficiency of the proposed algorithm SAODV, we have also plotted the original AODV protocol which can be considered as benchmark for the respective scenario. SAODV's performance has been analyzed to study the effect of mobility and scalability as well. The results have been shown for AODV without Blackhole (AODV-WOBH), AODV with Blackhole (AODV-WBH) and SAODV with Blackhole (SAODV-WBH).



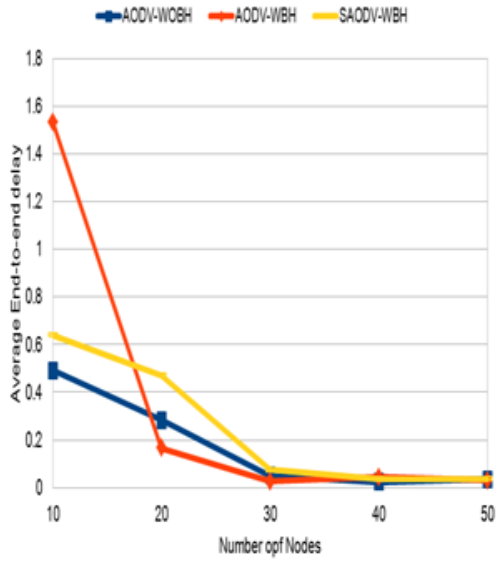
(a) Throughput vs. No. of Nodes



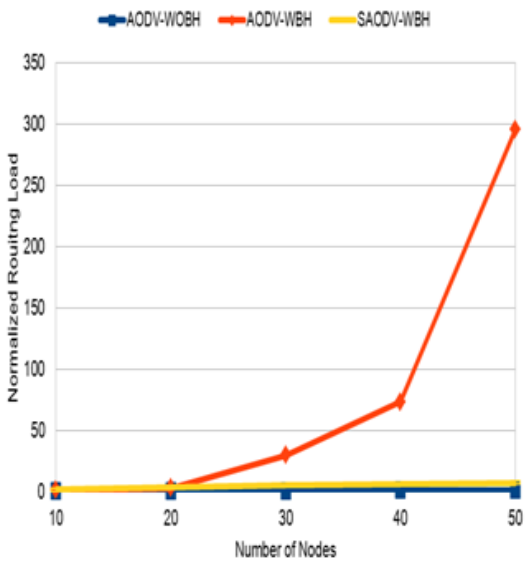
(b) PDR vs. No. of Nodes

- **Impact of scalability**

In the first experiment, we compare the performance of the protocols as the number of nodes in the network increases from 10 to 50 in the presence of 1 and 2 malicious nodes. The nodes move randomly with a maximum speed of 50m/s.



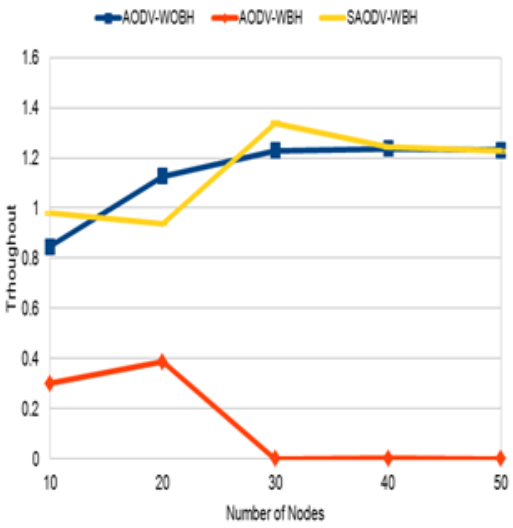
(c) Average end-to-end delay vs. No. of Nodes



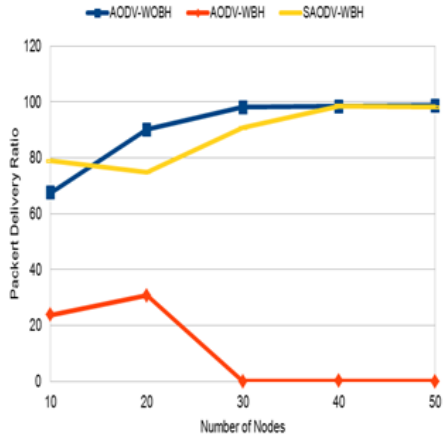
(d) NRL vs. No. of Nodes

Figure 6: Effect of scalability with 1 blackhole node

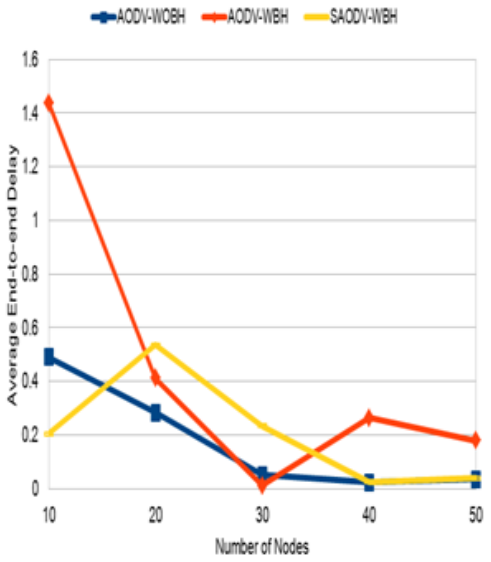
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



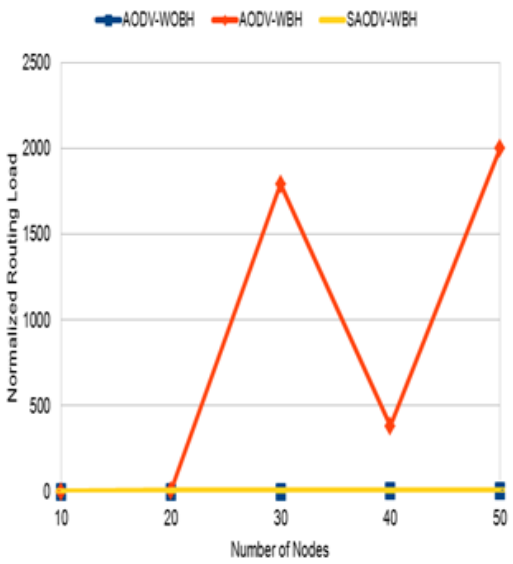
(a) Throughput vs. No. of Nodes



(b) PDR vs. No. of Nodes



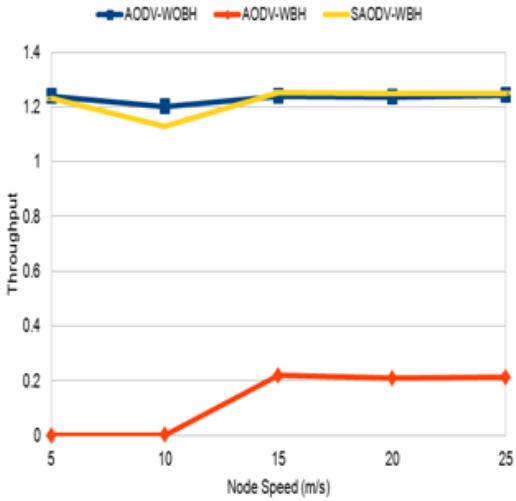
(c) Average end-to-end delay vs. No. of Nodes



(d) NRL vs. No. of Nodes

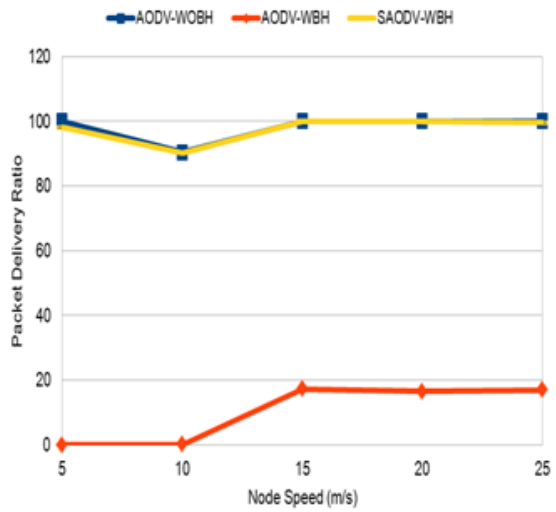
Figure 7: Effect of scalability with 2 blackhole nodes

- **Impact of mobility**
  In experiment 2, we evaluate the protocols by varying the maximum speed of nodes from 5m/s to 25m/s. The various performance graphs are plotted in fig. 4.10. An increase in node speed typically leads to frequent route breaks because of the increased link changes.

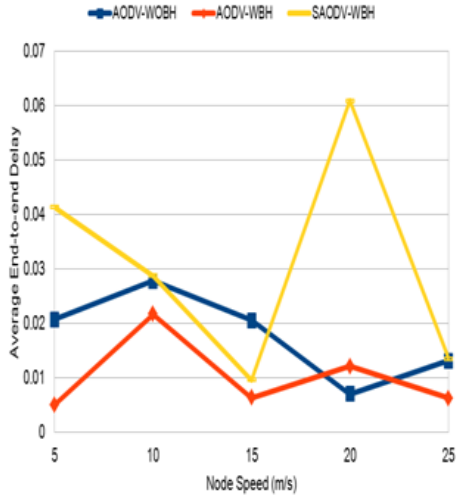


(a) Throughput vs. Node Speed

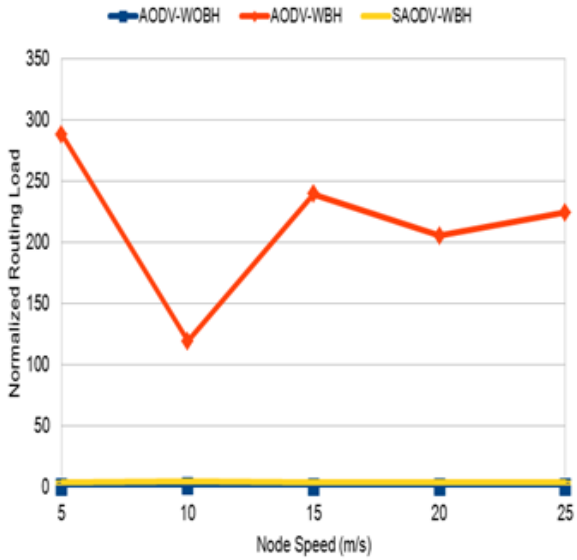
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



(b) PDR vs. Node Speed



(c) Average End-to-end Delay vs. Node Speed



(d) NRL vs. Node Speed

Figure 8: Effect of mobility with 3 blackhole nodes

Throughput: Effect of scalability and mobility on throughput is shown in fig. 6.(a), 7.(a) and 8.(a). SAODV achieves high throughput in comparison to original AODV routing protocol in presence of blackhole nodes. This is because it prevents malicious packet drops by black hole nodes. As throughput is a measure of how effective the protocol is, the results testify the same.

- Effect of scalability: With an increase in number of nodes, there is always an improvement in throughput of AODV and hence SAODV. However there is a decline in throughput of AODV in the presence of blackhole nodes. But with an increase in number of malicious nodes, throughput has declined slightly (fig. 7.(a))
- Effect of mobility: Regardless of the node speed, throughput of AODV shows a slight variation, because high mobility speed causes higher probability of link failures and in turn introduces more route discovery process. Our approach gave higher throughput as high as the benchmark (AODV-WBH).

PDR: Fig. 6.(b), 7.(b) and 8.(b) clearly shows that PDR of SAODV is equivalent to the benchmark in all scenarios, which is expected from any solution to ensure reliable data transmission. PDR is very high in SAODV because it is able to detect malicious node and enable source node to prevent the occurrence of black hole attacks. On the other hand, AODV gives poor PDR in presence of black hole nodes because maximum number of packets is consumed by the malicious node. The modified protocol improves the PDR by 60-80%.

- Effect of scalability: As the network size increases, there is a constant increase in the PDR of the proposed modification from 79.54 for 10 nodes to 98.3 for 50 nodes. Whereas there is a constant decline in the PDR of AODV in presence of blackhole nodes from 22.64 to 0.95.
- Effect of mobility: With mobility, SAODV shows a variation between 98-100%, which is same as that achieved by the original AODV.

Average End-to-end Delay: As shown in fig., SAODV has slightly more delay than AODV with an increase in network size and node speed. The increase in delay is due to processing overhead involved at the intermediate nodes as shown in fig. 4.(b), thereby taking more time to find a secure route. Hence, there will a tradeoff between delay and PDR. With small number of nodes, routing protocols take more time because of the limitation on the alternative routes. Results shown in fig. 6.(c), 7.(c) and 8.(c) shows the reliability of SAODV protocol with respect to delay.

- Effect of scalability: The delay decreases with increase in number of nodes. It is slightly more than the original AODV (benchmark). For instance, in presence of a single blackhole node, delay for 10 nodes is 0.491 of AODV and that of SAODV is 0.64054. The same effect is observed when

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

number of blackhole nodes was increased to 2.

- Effect of mobility: Overall, the delay decreases as the node speed increases. As said earlier, this delay is slightly more than the benchmark, which is acceptable in order to achieve security.

NRL: AODV has the lowest overhead since it doesn't use any control packets to discover secure routes; whereas SAODV uses extra control packets MHELLO and RMHELLO, thereby increasing the overhead. At the same time, it ensures more number of data packets reaching the destination successfully. As observed from the fig., NRL of AODV-WBH is highest due to the dropping of data packets by the black hole nodes. The NRL of SAODV with respect to varied node speed and network size is found to be more than AODV-WOBH because of extra control packets used. It is desirable to have a relatively stable NRL for scalability of the protocols, as it signifies that the actual routing load increases linearly with the number of sources.

- Effect of scalability: NRL is slightly more than the original AODV due to addition of control packets, but very less than AODV-WBH. With scalability, NRL of SAODV increases as presence of more number of nodes implies more transmission of control packets to check the reliability of a node.
- Effect of mobility: In presence of malicious nodes, hardly any data packets reach destination, thereby increasing NRL. However, though the number of control packets is more in SAODV but it ensures the successful transmission of data packets. Hence, it is more than AODV with increase in node speed.

Although many solutions exist to ensure security of MANETs against Blackhole attack; but none of them have achieved such high PDR and Throughput, with a very small amount of delay. It can be seen from the graphs that SAODV has accomplished more than 85-90% PDR in presence of any number of blackhole nodes, with a marginal increase in overhead and delay. There is a tradeoff between NRL and security when cooperative black hole exists. Hence we conclude that the proposed modification in AODV thereby provides high detection and prevention accuracy against single and collaborative black hole attack.

VI. CONCLUSION & FUTURE WORK

Having testified the susceptibility of AODV against Blackhole attacks, it is necessary to propose solutions to counter the Blackhole attack on AODV routing protocol. We have successfully demonstrated that with a minimal additional overhead of THRESHOLD variables and MHELLO packet, we are able to counter the effect. From the experimental results, we conclude that SAODV yields better performance in terms of Throughput, PDR, NRL and infinitesimal penalty in delay. Moreover, the proposed solution does not involve any hidden overhead on either the source nodes or the destination nodes. Consequently, in comparison to the other approaches discussed in section III, we believe the proposed algorithm is simple and efficient in implementation.

As part of our future work, simulations can be developed to analyze the performance of SAODV based on more parameters like memory usage, pause time, mean delay time etc. We aim to extend the proposed solution to secure AODV against other attacks such as Gray Hole attack, Wormhole attack etc.

REFERENCES

1. Nital Mistry, Devesh C Jinwala and Mukesh Zaveri, "Improving AODV Protocol against Blackhole attacks", Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol. 2, March 2010, Hong Kong.
2. C. E. Perkins, E. M. B. Royer and S. R. Das, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manetaodv- 00.txt, Feb. 2003.
3. C. Wahi, S.K. Sonbhadra, S. Chakraverty and V. Bhattacharya, "Effect of scalability and mobility on On-Demand routing protocols in a Mobile Ad-Hoc network", International Conference on Software and Computing Technology (ICSCT 2012), 21-22nd Dec'2012, Malaysia.
4. Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein, "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks", International Journal of Communication Networks and Information Security, Vol.3, No.1, pp-36-47, 2011.
5. H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, 40(10), pp. 70-75. doi:10.1109/MCOM.2002.1039859, 2002.
6. M. Al-Shurman, S-M. Yoo, and S. Park, "BlackHole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conf. 2004.
7. Tamilselvan, Latha and Sankaranarayanan, V. (2007). "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (Aus Wireless 2007) India, 2007 IEEE.
8. Sanjay Ramaswamy, Huirong Fu, and Kendall E. Nygard, "Simulation Study of Multiple Black Holes Attack on Mobile Ad Hoc Networks," International Conference on Wireless Networks (ICWN' 05), Las Vegas, Nevada, Jun. 2005.
9. Seryvuth Tan and Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-base MANETs", ICTC 2013.
10. Tamilselvan, Latha and Sankaranarayanan, V. (2008). "Prevention of cooperative black hole attack in MANET", in *Journal of Networks*, Vol. 3, NO. 5, MAY 2008.
11. Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathur and Prashant Khurana, "GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs", 27th International Conference on Advanced Information Networking and Applications Workshops, 2013.
12. Issariyakul, T., Hossain, E.: "Introduction to network simulation ns2," July 2008.