EFFICIENT MECHANISM FOR MITIGATING MULTIPLE BLACK HOLE ATTACKS IN MANETS

ABDUL-RAHMAN SALEM, DR. RUSHDI HAMAMREH
Computer Engineering Department
Al-Quds University, Jerusalem, Palestine
E-mail: asalem@outlook.com, rhamamreh@eng.alquds.edu

ABSTRACT

Mobile ad hoc networks (MANETs) have emerged as a major next generation wireless networking technology. Due to their inherent capabilities of instant communication, they are used for wide range of applications such as emergency operations and disaster recovery. On the other hand, many challenges are facing MANETs including security, routing, transmission range and dynamically changing topology with high nodes mobility. Security is considered as the main obstacle for the widespread adoption of MANET applications. Black hole attack is a type of DoS attack that can disrupt the services of the network layer. It has the worst malicious impact on network performance as the number of malicious nodes increases. Several mechanisms and protocols have been proposed to detect and mitigate its effects using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay. This paper proposes an enhanced and modified mechanism called "Enhanced RID-AODV", based on a preceding mechanism: RID-AODV. The proposed enhancement is based on creating *dynamic blacklists* for each node in the network. Each node, according to criteria depends on the number of mismatches of hash values of received packets as compared with some threshold values, can decide to add or remove other nodes to or from its blacklist. Enhanced RID-AODV was implemented in ns-2 simulator and compared with three previous solutions for mitigating multiple black hole attacks in terms of performance metrics. The results show an increase in throughput and packet delivery ratio and a decrease in end-to-end delay.

Keywords: *Enhanced RID-AODV, MANET Security, Network Layer Attack, Multiple Black Hole Attacks.*

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a self-configuring network formed by co-operating and independent nodes that connect and communicate with each other wirelessly without pre-existing infrastructure. If two mobile nodes are within each other transmission range, then they can communicate with each other directly; otherwise, the nodes in between have to forward the packet for them. So, mobile nodes are not only functioning as hosts but they are also functioning as routers [1].

Because MANETs are infrastructure-less networks with no centralized administration, they can be self deployed in short time. The easy deployment of nodes, self-organizing nature and freedom of mobility make MANETs suitable for a broad range of applications. They can be useful in disaster recovery and emergency operations where there is not enough time or resources to install and configure an infrastructure. They are also used in other applications; for example, in military services, maritime communications, vehicle networks, casual meetings, campus networks, robot networks… etc [2].

On the other hand, MANETs are vulnerable to various attacks at all layers. So, much research has been conducted on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. MANETs are vulnerable in their functionality: intruders can compromise the operation of the network by attacking at any of the physical, MAC or network layers. The network layer, especially the routing protocol, is vulnerable because of the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, the lack of clearly defined physical network boundary and the transient nature of services in the network. Standard information security measures such as encryption and authentication do not provide complete protection; thus, intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs [3].

Attacks in MANET can be divided, according to the criteria that whether they disrupt the operation of a routing protocol or not, into two classes: passive attacks and active attacks. In *passive attacks*, the attacker attempts to discover valuable information but does not disrupt the operation of the routing protocol. *Active attacks*;

however, involve actions like modification and deletion of exchanging data to absorb packets destined to other nodes to the attacker for analyzing or disabling the network. Some typical kinds of active attacks that can be performed against MANETs are: black hole attack, gray hole attack, flooding attack, selfish attack, rushing attack, spoofing, wormhole attack, sleep deprivation and impersonation [4].

Black hole attack is a type of active attack that exploits the route reply message (RREP) feature of the ad hoc on-demand distance vector (AODV) routing protocol. This attack involves some modification of the data stream or the creation of a false stream. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. A RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any other RREP messages from other neighboring nodes or even from the actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them [5].

So, the black hole attack is a DoS attack that disrupts the services of routing layer by exploiting the route discovery process of AODV. According to many research studies that focus on studying the effects of malicious attacks on network performance, the simulation results show that the black hole attack is more dangerous than other attacks in the network layer [6].

Several mechanisms and protocols have been proposed to detect and mitigate its effect using different strategies. However, many of these solutions impose more overhead and increase the average end-to-end delay.

In this paper, we propose a modified and enhanced protocol, called "Enhanced RID-AODV", based on a preceding mechanism: RID-AODV. It aims to detect and mitigate the effects of multiple black hole attacks in MANETs by increasing the throughput and packet delivery ratio (PDR) and by decreasing the end-to-end delay as compared to its predecessors. The proposed idea in this paper is creating a *dynamic blacklist* in each node, then prevent sending or forwarding to blacklisted nodes in both directions for a pre-specified period of time. The criteria to add a node in the blacklist is reaching a threshold in the number of mismatched hashing value from that node. The threshold is a function of mobility (*variable threshold*) to cancel the effect of normal link failure which is most likely caused by nodes mobility. The proposed solution, "Enhanced RID-AODV", was implemented in ns-2 simulator and compared with three previous solutions (namely RID-AODV, RAODV and IDSAODV) for mitigating multiple black hole attacks in terms of performance metrics. The results show an increase in throughput and packet delivery ratio and a decrease in end-to-end delay.

The rest of this paper is organized as follows: section II provides some details about the black hole attack, section III provides the related work in detection and mitigation of black hole attack. The proposed solution is introduced in section IV, the simulation and network environment are described in section V, in section VI, the analysis and the results are discussed. Finally, the conclusion is presented in section VII.

2. CLASSIFICATION OF SECURITY ATTACKS IN MANETS

Security attacks can be categorized, according to the criteria that whether they disrupt the operation of a routing protocol or not, into two broad classes: passive and active attacks. Passive attacks, where adversaries do not make any emissions, are mainly against data confidentiality. In active attacks, malicious acts are carried out not only against data confidentiality but also data integrity. Active attacks can also aim for unauthorized access and usage of the resources or the disturbance of an opponent’s communications. An active attacker makes an emission or action that can be detected [7][8].

The active attacks are generally launched by compromised nodes or malicious nodes. They are classified into four groups:

- *Dropping Attacks:* Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point, most of routing protocol has no mechanism to detect whether data packets have been forwarded or not.

- *Modification Attacks:* Black hole and Sinkhole attacks are example of modification and dropping attacks. These attacks modify packets and disrupt the overall communication between network nodes. In such attacks, the compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node then captures important routing information and uses it for further actions such as dropping or selective forwarding attacks.

- *Fabrication Attacks:* In fabrication attack, the attacker send fake message to the neighboring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages.

- *Timing Attacks:* In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique.

Malicious node may illegally modify the routing information of the received messages before forwarding them, it can alter one or several fields in the message, depends on the goals that it may want to achieve. The modification may include the route request (RREQ), route reply (RREP) and/or route error (RERR) as shown in table 1 below [9].

Table 1: Possible malicious modifications of routing protocols fields messages

Fields	**Messages**	**Modifications**
Type	All	Change the message type
Flags	All	Reverse the setting
Hop count	RREQ, RREP	Decrease it to update other nodes reverse route tables, or increase it to suppress its update
RREQ ID	RREQ	Increase it to make the faked RREQ message acceptable, or decrease it to make the RREQ message unacceptable
Dest_IP	RREQ, RREP	Replace it with another IP address
Dest_SEQ	RREQ, RREP	Increase it to update other nodes forward route tables, or decrease it to suppress its update
Orig_IP	RREQ, RREP	Replace it with another IP address
Orig_Seq	RREQ	Increase it to update other nodes reverse route tables, or decrease it to suppress its update
Prefix size	RREP	Increase/Decrease the size of the subnet prefix
Lifetime	RREP	Decrease/increase it to shorten/extend the lifetime of the route entry updated by this RREP message
Dest count	RERR	Modify it according to the number of unreachable destinations included in the RERR message
Un_Dest_IP	RERR	Replace it with another IP address
Un_Dest_SEQ	RERR	Increase it to update other nodes routing table, or decrease it to suppress this entry

3. BLACK HOLE ATTACK IN MANETS

Routing protocols in Mobile Ad Hoc Networks by their nature are distributed routing protocols with the assumption that all nodes in the network will cooperate truly and participate honestly. However, the existence of malicious nodes makes this assumption not true. Such nodes may drop the packets, if they are not the destination, without forwarding them or may disrupt the routing discovery and maintenance processes resulting in abnormal network operation that affects the performance of the network and may cause denial of service [10].

A black hole attack is a kind of denial of service (DoS) where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them (drop all packets) without forwarding them to the destination [11].

In reactive routing protocols such as AODV, the destination sequence number (*dest_seq*) is used to describe the freshness of the route. A higher value of *dest_seq* means a fresher route. On receiving a RREQ, an intruder can advertise itself as having the fresher route by sending a Route Reply (RREP) packet with a new *dest_seq* number larger than the current *dest_seq* number. In this way the intruder becomes part of the route to that destination [12]. Figure 1 illustrates the black hole attack where nodes S and D are the source and destination respectively and node B is the black hole.

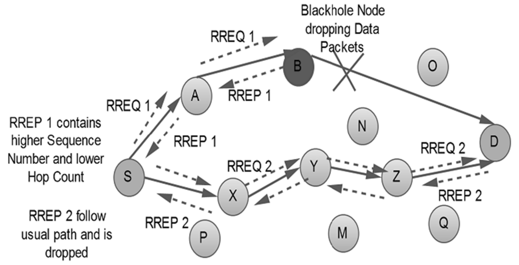

Figure 1: Black Hole Attack Illustration

A black hole has two properties: First, the node exploits the ad hoc routing protocol to advertise itself as having a valid route to a destination, even though the route is spurious with the intention of intercepting packets. Second, the node consumes the intercepted packets. In an ad hoc network that uses the AODV protocol, a black hole node absorbs the network traffic and drops all packets [11].

4. RELATED WORK

Some research studies in the literature have focused on studying the effect of malicious nodes on network performance only without providing any solutions. However, several mechanisms and protocols using different strategies have been proposed to protect MANETs against black hole attacks. In [6] the authors studied the effect of malicious attacks in mobile ad hoc networks including black hole attack, packet drop attack and gray hole attack on AODV protocol under different performance metrics: throughput, packet drop rate and end-to-end delay. It was found that the black hole attack is more dangerous than other attacks conducted in this paper.

Paper [13] provides a quantitative study of the performance impact of black hole attacks in ad hoc networks using DSR as the routing protocol. The authors used the following performance metrics to evaluate the impact of black hole attack on network performance: System Fairness, Number of hops for received packets, Total system throughput and Probability of interception. The simulation results of the impact of black hole node on system fairness showed that with no black hole node, the system has high fairness index.

In [14], authors analyzed the effects of black hole attack in mobile ad hoc network using AODV and DSR routing protocols. For the simulation, throughput was considered as the main measure. Though the simulation results showed a higher data packet loss when using DSR as compared to AODV, the dropped packet rate was still high for both protocols. DSR data loss was around 55 - 60 percent whereas that of AODV was around 45 - 50 percent. AODV protocol provides better performance than the DSR in the presence of black holes with minimal additional delay and overhead.

A black hole detection scheme for tactical MANETs using topology graph is proposed in[15]. This mechanism is called TOGBAD. It detects the attack using a topology graph, looking at the number of neighbors a node claims to have and the actual number of neighbors according to the graph. TOGBAD was developed for the OLSR proactive routing protocol, where topology information can be obtained.

Authors of [16] proposed an approach that uses improved security mechanisms to be introduced in the proposed techniques so that it satisfies the main security requirement and guarantees the discovery of a correct and secure route. The security mechanisms that the protocol uses are the hash chain, digital signature and Protocol Enforcement Mechanism. The performance of these two protocols (SAODV and ARAN) was tested in simulation and their communication costs were measured using the ns-2 simulator, which is suitable for the present purpose. The evaluation metrics used in this study were overhead and end-to-end delay. The results show good performance.

In [17] a proposed method was introduced to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is a large difference between the sequence number of source node or intermediate node that has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, then it is surely from the malicious node, immediately remove that entry from the RR-Table. The proposed method cannot find multiple black hole nodes.

In [18] the authors proposed and implemented a new intrusion detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to modern approaches, EAACK demonstrates privileged malicious behavior detection rates in definite situations while it does not greatly affect the network performances. The demonstrated results show positive performances.

A lightweight routing protocol IDSAODV was proposed in [19] as a solution for black hole attack problem in MANETs. The authors of [19] manually analyzed the output file obtained from simulation and found out very soon after the first RREP from the destination node a second RREP arrived at the source node. Through simulation, they found out that the first RREP was from the black hole node and the second RREP was from the intended destination. At this point, for future simulations, they assumed that the first RREP would always be from black hole node and modified the AODV protocol to ignore the first RREP and send using second RREP route. A RREP caching mechanism to count the second

RREP message was added to aodv.cc file in ns-2 simulator.

The simulation results of [19] demonstrate that IDSAODV improved the PDR in a MANET with a single black hole node; thus, proving the successful implementation of the route caching mechanism.

Many of the proposed solutions that make the route establishment process longer while the nodes are moving are facing from the link failure problem. In [5], the authors addressed this issue by getting advantage of the reverse AODV (RAODV) routing protocol proposed in [20]. RAODV discovers route using reverse route discovery procedure where the destination node sends reverse-route request (R-RREQ) messages to its neighbors to find a valid route to the source node after receiving RREQ from source node. Their simulation results of RAODV show that it does improve the performance of AODV in metrics such as packet delivery ratio (PDR), end-to-end delay, and energy consumption [20].

Although RAODV has not been designed to prevent black hole attacks and it was developed with the aim of solving path failure problem, authors of [5] proposed to use it in mitigating the effects of black hole attacks in ad hoc networks. So, they proposed RID-AODV by combining RAODV (proposed in [20]) and IDSAODV (proposed in [19]) to withstand multiple black hole attacks in client-based WMNs.

5. THE PROPOSED SOLUTION

The proposed protocol, "Enhanced RID-AODV", is a modification and enhancement of the RID-AODV protocol proposed in [5]. That protocol is based on RAODV [20] and IDSAODV [19] as mentioned in the previous section. Our solution is to get advantage of the nature of the reverse route discovery procedure in RAODV. The detection of the malicious nodes and mitigation their effects can be achieved by creating and maintaining *dynamic blacklist* in each node according to some criteria. Then each non malicious node will prevent sending or forwarding to the neighboring nodes that exist in its own blacklist either in the forward or reverse path In other words, each node will not use blacklisted nodes as intermediate nodes. Dynamic blacklist means that each node adds and removes nodes to or from its blacklist automatically according to specific criteria as will be explained in this section.

In addition, we can get another advantage of the nature of the reverse route discovery procedure in RAODV to create full path (bidirectional) integrity check implemented in hop-by-hop basis to detect any modifications on the traversing packets and to detect the causing nodes.

The criteria for each node to add another node's address in its blacklist is the repetitive mismatch in the hash value of the receiving frames (layer 2 frame) from the same neighboring node. So, each node keeps a counter for each other node that receives a frame from the neighboring nodes. If there is a mismatch between the received hash value and the calculated value, the corresponding counter for the sending (or forwarding) node will be incremented. When the counter reaches some threshold value $malPcktThreshold$, then the corresponding neighboring node will be blacklisted.

If node n_i has p neighboring nodes (p is $\subseteq$ of all nodes) and n_i is receiving from q nodes ($q\ is\ \subseteq\ of\ p$), then $n_i$will keep only q counters for this purpose. For example, for the network in figure 2, the node 9 will maintain less than or equal to 5 counters.

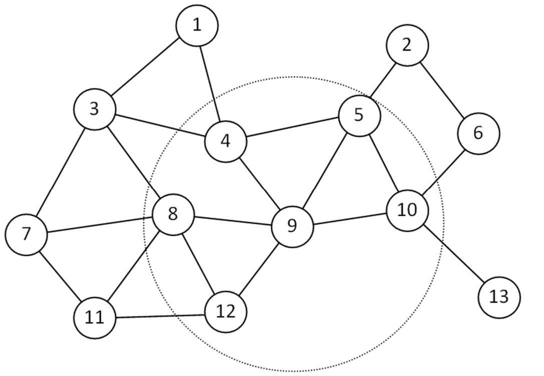

Figure 2: Each node maintains a small number of counters

To distinguish between hash value mismatch that may occur as a result of normal link failure, which is from the nature of MANETs due to mobility of nodes that communicate wirelessly, or from the existence of malicious nodes, the threshold value $malPcktThreshold$ should be considered as a function of mobility (*variable threshold*). If the node is moving with relatively high speed the mismatch of hash values is most likely due to normal link failure, and so the threshold should be high. On the other hand, if there are many hash value mismatches while the node is moving slowly, there is most likely a malicious node. So, the value of $malPcktThreshold$ is directly proportional to the node speed and it was implemented by using equation (1):

$$malPcktThreshold = NodeSpeed + C \qquad (1)$$

Where C is the threshold value when the node speed is zero.

The malicious node may not act as a black hole all the time, it may become benign for some period of time, then it may (or may not) resume its malicious activities. So, when a node adds another node's address to its blacklist, the blacklisted node will not stay in its blacklist forever. However, it will be blacklisted for a previously specified period of time. So, when a node is added to another node's blacklist, not only the address of the blacklist is added but also the expiry time for that node to be released from that blacklist. The blacklisted node expiry time is computed using equation (2):

$$blkListedNodeExpTime = CURRENT\_TIME + blocking\ Period \qquad (2)$$

Each time the node wants to send (or forward) a packet to a neighboring node, it will check if it is blacklisted, and if so it will also check the expiry time for that node. If it's expired, it will be removed from the blacklist of that node and its corresponding counter and expiry timer will be reset. Because of that it is dynamic blacklist.

Now when a node wants to send (or forward) a packet, in either the forward path or reverse path, it will check the routing table to decide what is the next hop. Then it will check if the next hop is blacklisted or not, if it's blacklisted, it will check the blacklist expiry time. If the next hop node is still blacklisted, then the node will remove that node from its neighbor list and run the handle link failure procedure. Then the node will try to send (or forward) the packet by using another path. Figure 3 and figure 4 are pseudo codes for the proposed solution. Figure 3 describes how the node decides to add or remove other nodes to or from its blacklist, and figure 4 how the node behaves when sending or forwarding a packet.

Pseudo code for the proposed solution: How the node decides to add or remove other nodes in its blacklist:

```
1. Generate new hash value ($NewHash$).
2. Compare the generated hash value $New\_Hash$ with the received hash value with the packet $HashVal$.
3. if($NewHash \neq HashVal$)
   then, $incr\ malNodeCouter(PrevHopAddr)$
4. Check the speed of the node ($NodeSpeed$).
5. Compute the threshold that will be used to consider a node as blacklisted
      $malPcktThreshold = NodeSpeed + C$
6. //To add a node to a blacklist
   if(isBlacklisted(NextHop) == FALSE &&
     $malNodeCouter(NextHop) > malPcktThreshold$)
   then,
      a. $addBlackList(NextHop)$.
      b. $blkListedNodeExpTime(NextHop) = CURRENT\_TIME + Blocking\ Period$
7. //To remove a node from a blacklist
   else if(isBlaklisted(NextHop) == TRUE &&
     $CURRENT\_TIME > BlkListedNodeExpTime(NextHop)$)
   then,
      a. $removeBlackList(NextHop)$.
      b. $malNodeCouter(NextHop) = 0$
      c. $blkListedNodeExpTime(NextHop) = 0$
   //For other cases: keep the blacklist as it is
```

Figure 3: Pseudo code for the proposed solution: How the node decides to add or remove other nodes in its blacklist

Pseudo code for the proposed solution: How the node behaves when sending or forwarding a packet:

```
1. if(isBlacklisted(NextHop) == TRUE)
   then,
      a. // Delete blacklisted node from neighbors list
         $nb\_delete(NextHop)$
      b. //Consider link with blacklisted node as link failure
         $handle\_link\_failure(NextHop)$
```

Figure 4: Pseudo code for the proposed solution: how the node behaves when sending or forwarding a packet

6. SIMULATION AND NETWORK ENVIRONMENT

The simulation was carried out using ns-2 simulator under Ubuntu Linux operating system. Ns-2 is a discrete-event simulator that is written in C++, which is object oriented language. During the simulation the packet header (aodv_packet.h file) of the AODV route request and route reply (changed to route reverse request) are modified to hold the hash value ($Hash\_Val$) with packet. In addition to that, the files aodv.h and aodv.cc were modified to implement the proposed solution together with previous protocols. Simulation was done by referring to many resources including but not limited to [21][22][23].

The simulation area is a square field of 1000m x 1000m with fixed sender and receiver nodes that communicate using intermediate mobile nodes, which are moving randomly during simulation time (these random movements were generated using '*setdest*' tool) and are sending random traffic pattern among each other (created using '*cbrgen.tcl*' command). The sender and receiver were placed in points (200,200) and (800,800) respectively. The parameter considered in this simulation is given in table 2 below.

TABLE2: PARAMETERS USED IN NS-2 SIMULATION

Parameter	Value
Simulator	ns-2
Routing protocol	AODV, IDSAODV, R-AODV, RID-AODV, Enhanced RID-AODV
Simulation time	100 sec
Simulation area	1000m x 1000m
Number of nodes	40
Number of malicious nodes	0,1,2,3,4,5,6,7
Sender node	Fixed at point (200,200)
Receiver node	Fixed at point (800,800)
Intermediate nodes	Moving randomly
Maximum speed of mobile nodes	20 m/s
Data Rate	50 Kb/s
Pause time	0 sec
Transport type	UDP, CBR
Data packet size	Default
MAC Protocol	IEEE 802.11

In this research, the proposed solution together with four preceding protocols were implemented and simulated with the same environment parameters to be able to make a comparison among them. That include: the genuine AODV protocol with simulation of black hole malicious nodes, the IDSAODV protocol proposed in [19], RAODV proposed in [20], RID-AODV that was proposed on [5] and our proposed solution in this paper which is Enhanced RID-AODV. For each protocol many scenarios were generated to simulate the existence of different number of malicious nodes in order to study the effect of multiple malicious nodes on network performance and the effectiveness of each solution to compare among these solutions; we made as many combinations of nodes to act as malicious nodes and then we computed the average of the results.

Performance Metrics:

In this simulation, the following three performance metrics were considered and computed as the average of many cases in all scenarios of multiple malicious nodes for all the protocols in the study. Three separate scripts were generated to compute these performance metrics using *awk* command.

- **Throughput:** The amount of data transferred over the period of time expressed in kilobits per second (kbps). Throughput has been calculated using equation (3):

$$Throughput = \frac{\sum Size\ of\ Received\ Data\ Packets}{Simulation\ Time} \quad (3)$$

- **Packet Delivery Ratio (PDR):** The percentage ratio of the total number of data packets received by the destination node to the number of data packets sent by the source node as in equation (4).

$$PDR = \frac{\sum Number\ of\ Received\ Data\ Packets}{\sum Number\ of\ Sent\ Data\ Packets} * 100\% \quad (4)$$

- **Average End-to-End Delay:** The average delay between the sending of the data packet by the source node and its receipt at the destination node. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer… etc. The average end-to-end delay was computed using equation (5).

$$Avg\_E2E\_Delay = \frac{\sum_i (Receive\ Time\ of\ P_i - Sent\ Time\ of\ P_i)}{Number\ of\ Received\ Packet} \quad (5)$$

7. RESULTS AND ANALYSIS

Simulation results show that only one black hole in the network - without any solution - is able to decrease the PDR to almost 10% of its value without black hole. And only a small number of black holes in the network are able to reduce the throughput and the packet delivery ratio to almost zero resulting in denial of service (DoS) for the legitimate nodes, as illustrated in figure 5 and figure 6 respectively.

These two figures also show the results of applying four solutions: IDSAODV, R-AODV, RID-AODV and the proposed Enhanced RID-AODV on increasing the throughput and the packet delivery ratio. It's obvious that the proposed protocol "Enhanced RID-AODV" has the highest throughput and the packet delivery ratio. That happens because of the effect of applying the dynamic blacklists with variable threshold resulting in reducing the packet loss due to malicious nodes.

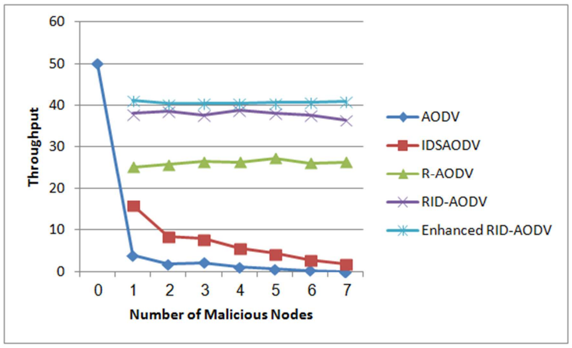

Figure 5: Effect of number of malicious nodes on Throughput for different protocols in mitigating multiple black hole attacks

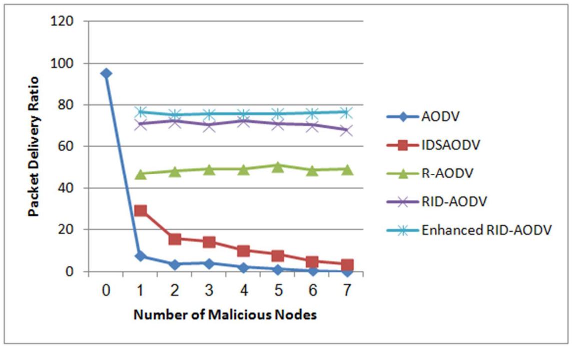

Figure 6: Effect of number of malicious nodes on Packet Delivery Ratio for different protocols in mitigating multiple black hole attacks

Another major improvement as a result of applying the proposed protocol is decreasing the average end-to-end delay; that because of the effect of the dynamic blacklists in forwarding packets to only the non malicious intermediate nodes to create right paths and to avoid the malicious nodes in both the forward and reverse paths. This is clear in figure 7 below.

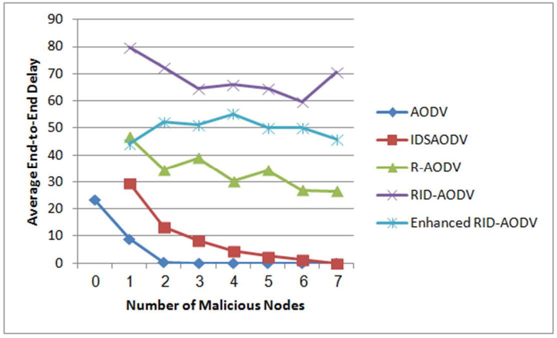

Figure 7: Effect of number of malicious nodes on Average End-to-End Delay for different protocols in mitigating multiple black hole attacks

8. CONCLUSION

In this paper a new mechanism, called "Enhanced RID-AODV", was proposed to detect and mitigate the effects of multiple black hole attacks in MANETs. It is an enhanced and modified version of a previously proposed mechanism called RID-AODV. RID-AODV is a combination of reverse routing and route caching technique. The proposed idea in this paper is creating a dynamic blacklist in each node, then prevent sending or forwarding to blacklisted nodes in both directions for a pre-specified period of time. The criteria to add a node in the blacklist is reaching a threshold in the number of mismatched hashing value from that node. The threshold is a function of mobility (variable threshold) to cancel the effect of normal link failure which is most likely caused by nodes mobility. According to the simulation results, Enhanced RID-AODV provides higher throughput and higher packet delivery ratio than its preceding version. Also, the dynamic blacklists provide positive effects in decreasing the end-to-end delay.

REFERENCES

[1] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC: 2501, IETF. [Online]. Available: http://tools.ietf.org/html/rfc2501

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, “A Survey Of Routing Attacks In Mobile Ad Hoc Networks,” IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007.

[3] A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE Communications Surveys & Tutorials, 2013.

[4] S. Behzad and S. Jamali, "A Survey over Black hole Attack Detection in Mobile Ad hoc Network", International Journal of Computer Science and Network Security (IJCSNS), Vol.15 No.3, March 2015

[5] O. Shree, F. J. Ogwu, "A Proposal for Mitigating Multiple Black-Hole Attack in Wireless Mesh Networks", Wireless Sensor Network, vol. 5, no. 4, pp- 76-83, 2013.

[6] A. Kanthe, D. Simunic , R. Prasad, "Effects of Malicious Attacks in Mobile Ad-hoc Networks", 2012 IEEE International Conference on Computational Intelligence and Computing Research, ISBN:978-1-4673-2481-6,18-20, December 2012, Coimbatore, India.

[7] E. Cayirci and C. Rong, "security in wireless ad hoc and sensor networks". John Wile and Sons, 2009

[8] A. Saeed, A. Raza and H. Abbas, "A Survey on Network Layer Attacks and AODV Defense in Mobile Ad Hoc Networks", IEEE Eighth International Conference on Software Security and Reliability, SERE 2014, USA 2014

[9] A. K. Abdelaziz, N. Mehdi and G. Salim, "Analysis of security attacks in AODV", International Conference on Multimedia Computing and Systems(ICMCS), (2014)

[10] H. Ehsan and F. A. Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs". 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2012.

[11] L. Tamilselvan and V Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET" JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008

[12] S. kurosawa and A. Jamalipour, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, Nov 2007.

[13] I. Aad, P. J. Hubaux and W. E. Knightly, "Impact of Denial-of-Service Attacks on Ad-Hoc Networks," IEEE-ACM Transactions on Networking, Vol. 16, No. 4, 2008, pp. 791- 802.

[14] D. Mishra, K. Y. Jain and S. Agarwal, "Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)", Proceeding from ACT'09: IEEE Advances in Computing, Control and Telecommunication Technologies, Trivandrum, 28-29 December 2009, pp. 621-623.

[15] E. Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", Proc. IEEE Conference on Local Computer Networks, 2007.

[16] D. Wadbude, V. Richariya, "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, 2012, pp. 274-279

[17] L. Himral, V. Vig and N. Chand, "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[18] M. Shakshuki, N. Kang and Sheltami,"EAACK- A Secure Intrusion-DetectionSystem for MANETs", IEEE Transactions on Industrial Electronics, vol. 60, no. 3, March 2013.

[19] S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.

[20] C. Kim, E. Talipov, and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks", The International Conference on Emerging Directions in Embedded and Ubiquitous Computing (EUC'06), Seoul, 1-4 August 2006, pp. 522-531. Springer, 2006.

[21] The Network Simulator ns-2. [Online]. Available: http://www.isi.edu/nsnam/ns

[22] N. Hegde and S. Manvi, "Simulation of Wireless Sensor Network Security Model Using NS2", International Journal of Latest Trends in Engineering and Technology (IJLTET). Vol. 4 May 2014

[23] C. Manikandan, R.Parameshwaran, K.Hariharan, N.Kalaimani and K.P. Sridhar, "Combined Security and Integrity Agent Integration into NS-2 for Wired, Wireless and Sensor Networks" Australian Journal of Basic and Applied Sciences, 7(7): 376-382, 2013 ISSN 1991-8178