A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs

Tarek M. Mahmoud
Faculty of Science,
Computer Science Department,
Minia University,
Minia, Egypt

Abdelmgeid A. Aly
Faculty of Science,
Computer Science Department,
Minia University,
Minia, Egypt

Omar Makram M.
Faculty of Science,
Computer Science Department,
Minia University,
Minia, Egypt

ABSTRACT

Mobile ad hoc networks (MANETs) are composed of a set of stations (nodes) communicating through wireless channels, without any fixed backbone support in which nodes are allowed to join and leave the network at any point of time. MANETs are generally more vulnerable to information and physical security threats than wired networks, so security is an essential requirement in MANETs to provide secured communication between mobile nodes. One of the most common attacks against routing in MANETs is the Black Hole attack. A black hole is a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In this paper, we attempt to focus on improving the security of one of the popular routing protocol for MANETS, namely the Ad hoc On Demand Distance Vector (AODV) routing protocol to avoid black hole attacks. The proposed Intrusion Avoidance System (IASAODV) can be considered as modification of the AODV protocol and can be used to detect and avoid the black hole attack. The conducted experimental results using Network Simulator NS-2.35 show an improvement in Packet Delivery Ratio (PDR), Normalized Routing Load (NRL) and throughput using the proposed protocol compared with AODV routing Protocol in the case of existing black hole attack.

Keywords

MANETs, AODV Routing Protocol, IASAODV Protocol, Black Hole Attack and NS2.

1. INTRODUCTION

A MANET is a collection of mobile nodes that cooperatively and spontaneously form a wireless network without the use of any fixed infrastructure (e.g., base stations or access points), or centralized administration. The system may operate in isolation, or may have gateways connected with a fixed network. In the latter mode, it is typically envisioned as a sub network connected to a fixed network. The mobile devices used in ad hoc networks could include an evolution of current cell phones, PDA, or laptops equipped with wireless interfaces. Securing MANETs routing faces difficulties which do not exist in wired networks, nor in infrastructure-based wireless networks [1]. These difficulties make trust establishment among nodes virtually impossible. Among these difficulties are the wireless medium itself and its physical vulnerability, the lack of centralized control and permanent trust infrastructure, the cooperation of nodes, restricted power and resources, highly dynamic topology and short-lived connectivity and availability. However, there are still many open issues about MANETs, such as security problem, finite transmission bandwidth, abusive broadcasting messages, reliable data delivery, dynamic link establishment and restricted hardware. In the following, we briefly introduce the widely-used requirement to ensure the real-time communications security of MANETs [2]:

*Integrity***,** Integrity of data ensures that a packet is not modified during transmission. This requires data authentication. Without integrity, attackers can easily corrupt and modify the data and therefore cause mobile devices to make wrong decisions based on the corrupted data.

Authentication is the process to verify the identity of the sender of a communication. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. Without authentication, malicious attackers can access resource, gain-sensitive information, and interfere with the operation of other nodes very easily.

Confidentiality means certain information is only accessible to authorized recipients. Participating parties to handle an emergency event need to cooperate with each other, while keeping the confidentiality of the traffic traversing the network.

Non-repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. It is useful for detection and isolation of compromised nodes.

Availability ensures the survivability of network services despite denial of service attacks (DoS). In unreliable wireless communications with highly dynamic topology, availability affects network performance greatly.

The security threats have been extensively discussed and investigated in the wired and wireless networks. The correspondingly perplexing situation has happened in MANET due to the inherent design defects there are many security issues which have been studied in recent years. For instance, snooping attacks, wormhole attacks, black hole attacks, routing table overflow and poisoning attacks, packet replication, Denial of Service (DoS) attacks [3]. Black hole attacks can be considered one of the popular attacks that belong to DoS attacks. From security point of view, multiple lines of defense against attacks are desired. A complete security solution for wireless ad hoc networks should contain three components: prevention, detection, and reaction [4]. In this paper, we focus on analyzing and improving the security of the AODV routing protocol against the black hole attacks. A modified routing protocol is proposed to detect and avoid black hole attacks. The reminder of this paper is organized as follows: Section 2 describes the AODV routing protocol. The black hole attack is described in Section 3. Section 4 discusses the related works. The modified routing protocol and its implementation are given in Section 5. Section 6 introduces the experimental results. Finally, Conclusion & Future work are given in Section 7.

2. AODV ROUTING PROTOCOL

AODV routing protocol is a reactive routing protocol for the MANET that maintains routes only between nodes that need to communicate each other [5].

The routing messages do not contain information about the whole route path, but only about the source and the destination information. Therefore, the routing messages do not have an increasing size. It uses the Source Sequence Number (SSN) or the Destination sequence number (DSN) to specify how fresh a route is, which is used to grant loop freedom. The following subsections give a brief description of how routes are built and maintained in MANETs. Neighbor connectivity is established with periodic Hello Messages. Routes are found by flooding of route request (RREQ) messages as can be seen in Figure 1(a). As each node receives and retransmits the RREQ it records the previous hop in its routing table. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. A timer call RREP_WAIT_TIME is started when the RREQ is sent. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP), as can be seen in Figure 1 (b), to the source node through the reverse path where the RREQ arrived. The destination node will ignore the same RREQ that arrives later. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node. Once the source receives the first RREP message, it starts the data transmission along the path traced by the RREP packet.

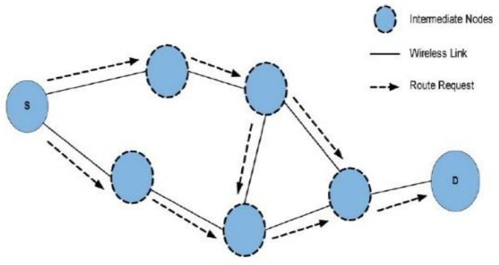

Figure 1(a). RREQ message

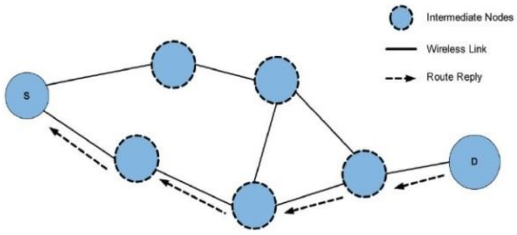

Figure 1(b). RREP message

AODV provides a rapid, dynamic network connection, featuring low processing loads and low memory consumption. AODV uses a node sequence number to distinguish whether the routing message is fresh or not. Node sequence numbers serve as time stamps and allow nodes to compare how fresh their information on the other node is. However when a node sends any type of routing control message such as RREQ and RREP it increases its own sequence number. Higher node sequence number means that the fresh route to the destination can be established over this node by other nodes. Routing messages in a network can be divided into path discovery and path maintenance messages. Path discovery includes RREQ and RREP, while path maintenance includes Route error (RERR) and Hello messages. Since the RREQ and RREP are directly and largely involved in the modified routing protocol suggested in this paper, their formats are shown in Table 1 and Table 2, respectively.

Table 1. RREQ message format

Type	Flags	Reserved	Hop count
RREQ (Broadcast) ID			
Destination IP address			
Destination sequence number (DSN)			
Source IP address			
Source sequence number (SSN)			

Table 2. RREP message format

Type	Flags	Reserved	Hop count
Destination IP address			
Destination sequence number (DSN)			
Source IP address			
Source sequence number (SSN)			

When a new route is available, the routing table will be updated only if this new route has larger destination sequence number or same destination sequence number with smaller hop count to the destination node. Each routing table entry contains the following:

- Destination IP address
- Next hop
- Number of hops
- Destination sequence number
- Active neighbors for this route
- Expiration time for the route table entry

3. BLACK HOLE ATTACK IN AODV

A black hole attack is one of the active DoS attacks possible in MANETs [6]. In this attack, a malicious node may advertise a fresh path to a destination during routing process. The intention of the node may be to disturb the path finding process or interpret the packet being sent to destination. For example, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Since AODV treats RREP messages having higher value of destination sequence number to be fresher, the malicious node will always send the RREP having the highest possible value of destination sequence number. Such RREP message, when received by source node is treated a fresh route. An example of black hole attack is shown as Figures 2(a) and 2(b) in which nodes S and D represent the source and the destination nodes respectively.

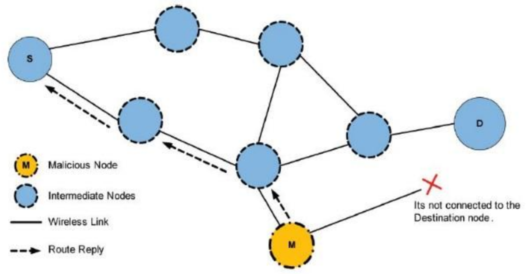

Figure 2(a) A malicious node sending false RREP to the source node

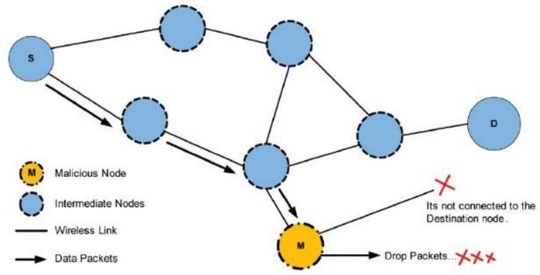

Figure 2(b) A malicious node dropping data packets as the source node is unaware

Node M is a malicious node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node S erroneously judges the route discovery process with completion, and starts to send data packets to node M. As what mentioned above, a malicious node probably drops or consumes the packets. This malicious node can be regarded as a Black Hole problem in MANETs.

4. RELATED WORK

The black hole attack problem has attached the attention of many researchers. Many algorithms have been proposed to solve this problem. These algorithms are either completely new stand-alone protocols, or in some cases incorporations of security mechanisms into existing protocols (e.g. AODV). As we will see, the design of these solutions focuses on providing countermeasures against black hole attack. In this section we introduce some of the existing algorithms used to avoid the black hole attack.

Chin et al [7] proposed a specification-based intrusion detection system that can detect attacks on the AODV routing protocol. They used finite state machines for specifying correct AODV routing behavior and distributed network monitors for detecting run-time violation of the specifications. In addition, they proposed one additional field in the protocol message to enable the monitoring.

Nishant Sitapara et al [8] presented an intrusion detection system for AODV protocol (IDSAODV) for single Black Hole attack. They used an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals assuming that the first RREP message arrived from the black hole node.

Lalit, et al [9] proposed an efficient algorithm for preventing AODV routing protocol from black hole attack in the MANETs. This algorithm can be used to find the secured routes and prevent black hole nodes by the identifications of the nodes with their sequence number. The identification is made for whether there is large difference between the sequence number given by the source node and the sequence number given by the intermediate nodes who has sent back RREP message. When the malicious node is identified, the routing table information sent from the malicious node, are discarded from the network. The advantage of this algorithm that is improving the packet delivery ratio compared with original AODV.

Ming-Yang [10] proposed an Intrusion Detection System (IDS) to solve the selective black hole attacks in MANET based on Anti-black hole mechanism (ABM). Since there is no centralized infrastructure device in MANET, it’s challenged to develop an intrusion detection system (IDS). All IDS nodes perform an ABM, which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS’s suspicious node (SN) table. When the suspicious value of a node exceeds a threshold, a block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node.

Jan von Mulert et al [11] discussed security threats and solutions in MANETs. They focused on networks using the popular AODV protocol and a secure extension to AODV, the Secure AODV (SAODV) protocol. SAODV is representative of a number of secure versions of the AODV protocol in that it relies upon the use of cryptographic mechanisms to protect the routing control messages of AODV from being forged and/or altered by attackers. They conducted a vulnerability analysis of SAODV to identify unresolved threats to the algorithm, such as black holes attacks.

Shashank et al [12] suggested a solution that is an enhancement of the basic AODV routing protocol used to avoid Black Hole attacks.

[13], [14], [15] and [16] introduced the simulation the AODV routing protocol under black hole attack and the analysis of it is effect. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. The result shows significant degradation in performance of ad hoc on demand vector routing protocol (AODV) under black hole attack. The packet dropping clearly shows that black hole attack has occurred. Simulation results show that the throughput is decreased with black hole attack as compared to without black hole attack.

5. THE PROPOSED ALGORITHM

The proposed algorithm is designed to prevent any alterations in the default operations of either the intermediate nodes or the destination nodes. After analyzing the effect of black hole attack in MANETS, we modify the AODV Protocol and propose a detection technique called Intrusion Avoidance System (IASAODV), which helps to detect and avoid the black hole nodes.

The proposed algorithm is divided into major stages:

- The first stage is based on the routing messages of both RREQ and RREP messages that are exchanged in the route discovery.
- The second stage is based on the DSN of the RREP message, the number of RREP message(s) calculated in the first stage and the arrival time of RREP at the source.

The first stage of the proposed algorithm includes monitoring all the RREQ and RREP messages between the source and destination nodes. A Route Reply Table (RRT) is created to store any RREP message(s) from destination node.

As mentioned above, black hole node sends a fake RREP message with maximum node sequence number to the source node in order to pose itself as a destination or an intermediate node. So, the source node sends data to it. To avoid this process, we consider that the source node must wait a time equals the double value of RREP_WAIT_TIME, before sending data, in order to receive more RREP messages. Once the source node receives the RRRP message(s) it will store its sequence number and the time at which the message(s) arrives in a table. In our implementation we refer to this table by Route Reply Table (RRT).

Throughout the second stage, when the source node receives the RRRP message(s) it will store its destination sequence number and the arrival time in RRT. When the timer RREP_WAIT_TIME expires, then the proposed algorithm checks the number of RREP messages in RRT.

The emergence of more than one RREP message means there is a threat of black hole attack. In the case of receiving only one RREP message, the destination node is considered trusted node and all data will be send to it. Receiving more than one RREP message means that one of these messages is created by the trusted destination node and the other message(s) are created by black hole node(s).

The Pseudo-code of the proposed algorithm can be described as follows:

```
Receive Reply (Packet P)
    Reply_count= 0
    initiate Route Discovery ( )
Set time (RREP_WAIT_TIME) ← double value of
RREP_WAIT_TIME
        While ( received _RREP)
        {
              insert RREP into RRT
              Reply_count ← Reply_count + 1
         }
If  Reply_count=1                // RRT contains the trusted node
      then
            Unicast data packets from the source node to the
            trusted  destination node
     else                        // RRT contains black hole node(s)
          {
           Select the RREP message with minimum DSN
         // the node with minimum DSN is considered trusted
         // destination node, otherwise is considered black hole
         // node(s)
               Unicast data packets from the source node to the
               trusted  destination node.
           }
```

6. SIMULATION'S RESULTS

The conducted simulation experiments were performed using NS-2 Ver. 2.35 simulator [17] and [18] run on Intel Core i3 to validate the detection and isolation efficiency of the proposed algorithm against black hole nodes. The simulation models a network of 15, 20, 25, 30, 35, 40, 45 and 50 mobile nodes migrating with square area size 750 x 750 m^2. The mobility model uses the random waypoint (RWP) model in the considered area. In this, each node is randomly placed in the simulated area and remains stationary for a specified pause. We chose out traffic sources to be Constant Bit Rate (CBR). Each CBR packet size is 512 bytes. Table 3 shows the main simulation parameters used for scenarios.

Table 3. Simulation Parameters

Parameter	**Value**
Simulator	NS-2 (Ver. 2.35)
Simulation Time S	500 sec
Number of mobile nodes	15,20,25,30,35,40,45 and 50
Number of Black hole nodes	1,3 and 5 nodes
Simulation area	750 m X 750 m
Transmission range	250 m
Routing Protocol	AODV & IDSAODV & proposed IASAODV
Traffic Type	Constant Bit Rate (CBR)
Maximum Speed	20 m/s
No. of Connection between nodes	10
Packet Size	512 bytes
Mobility Model	Random Way point
Data Rate	4 Mbps
RREP_WAIT_TIME	2 sec

In order to evaluate the performance of the proposed algorithm, we compare it with both AODV and IDSAODV protocols. The packet delivery ratio PDR, normalized routing load, average End-to-End Delay and average throughput has been used to analyze the performance of considered routing protocols. *PDR* is defined as the ratio of the data packets received at the destination station compared to the total of data packets transmitted by the source node. *NRL* is defined as the Number of routing packets "transmitted" per data packet "delivered" at destination node. Each hop-wise transmission of a routing is counted as one transmission. It is the sum of all control packet sent by all nodes in network to discover and maintain route. *The Average End-to-End Delay* is defined as the average time employed for a data packet to be delivered from the source node to the destination node. *The Average Throughput* is defined as the sum of the data delivered to all the nodes in the network in a given time unit (seconds). Three simulation scenarios are considered.

A. One black hole attack scenario.

A. Three black holes attack scenario.

B. Five black holes attack scenario.

A. Scenario 1

Figures 4, 5, 6 and 7 represent the simulation results of the considered protocols. In each Figure, the number of nodes is considered versus normalized routing load, packet delivery ratio, average throughput and average end-to-end delay respectively.

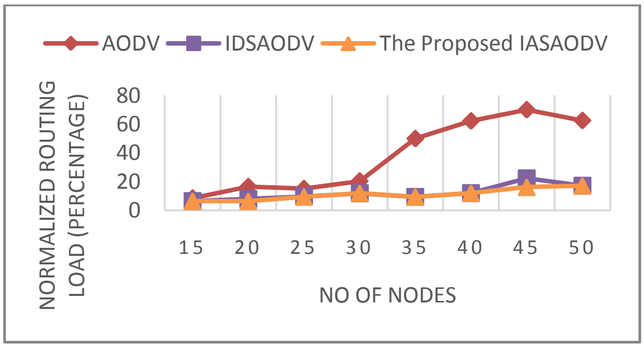

Figure 4: number of nodes vs Normalized Routing Load in case of one black hole node attack.

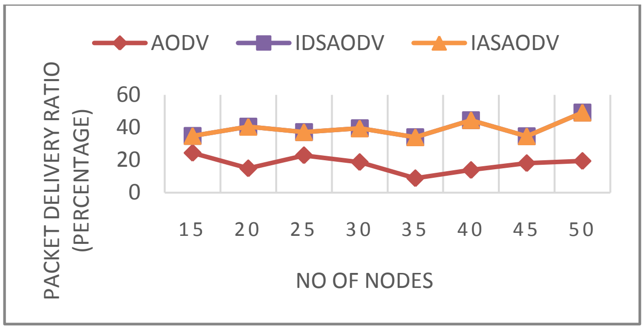

Figure 5: Number of nodes vs Packet Delivery Ratio in case of one black hole node attack

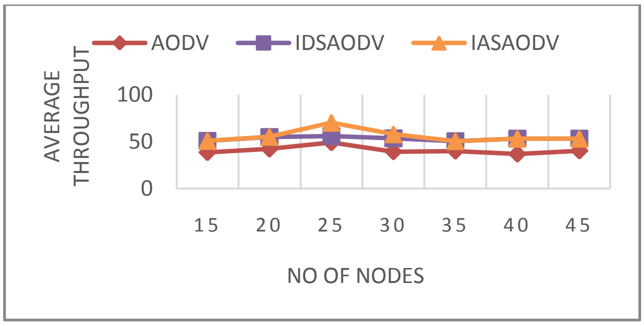

Figure 6: Number of nodes vs Average Throughput in case of one black hole node attack

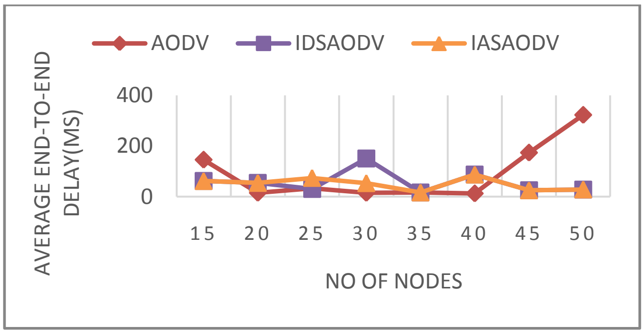

Figure 7: number of nodes vs Average end-to-end delay in case of one black hole node attack

From previous Figures, it can be observed that, in the case of one black hole node attack, the packet delivery ratio of the proposed IASAODV and the IDSAODV is better than the AODV. The normalized routing load for the proposed IASAODV better than both AODV and IDSAODV protocols. The average throughput of both the IDSAODV and the proposed IASAODV is better than the AODV protocol. In general, the average end-to-end delay of the AODV protocol is less than both the IDSAODV and the proposed IASAODV protocols due to the doubled waiting time.

B. Scenario 2

Figures 8, 9, 10 and 11 represent the simulation results of the considered protocols. In each Figure, the number of nodes is considered versus normalized routing load, packet delivery ratio, average throughput and average end-to-end delay respectively.

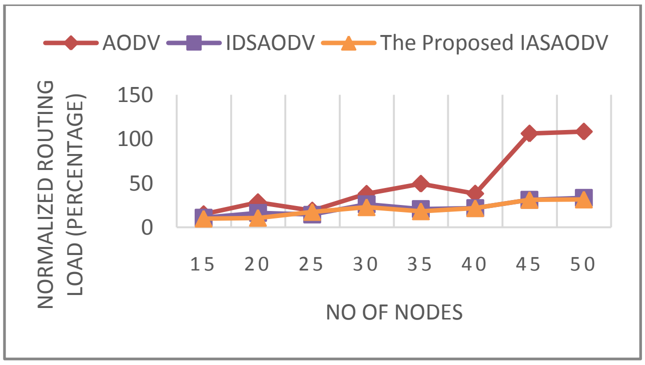

Figure 8: number of nodes vs Normalized Routing Load in case of three black hole nodes attack.

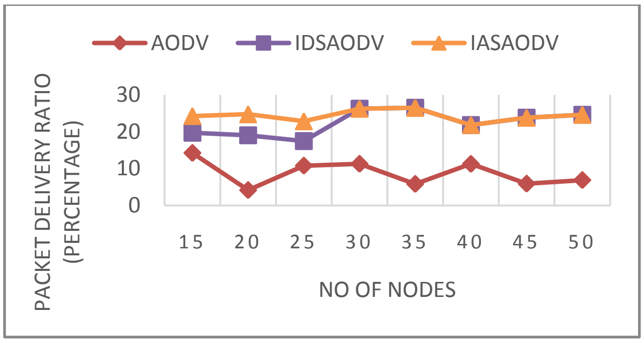

Figure 9: Number of nodes vs Packet Delivery Ratio in case of three black hole nodes attack

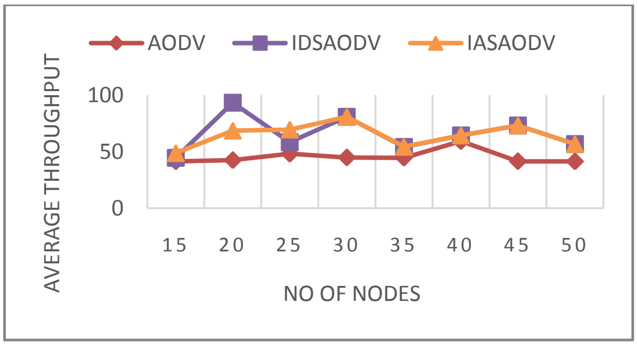

Figure 10: number of nodes vs Average Throughput in case of three black hole nodes attack

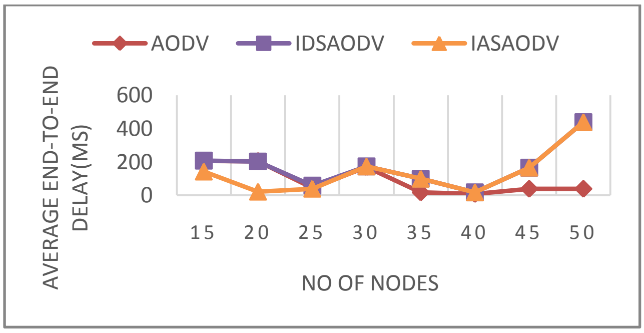

Figure 11: number of nodes vs Average end-to-end delay in case of three black hole nodes attack

As can be seen in these Figures, in the case of three black hole nodes attack. The packet delivery ratio and normalized routing load of the proposed IASAODV protocol is better than both AODV and IDSAODV protocols as the number of nodes is increased. Starting with 30 nodes, the packet delivery ratios of both the proposed IASAODV and IDSAODV have the same values and are better than AODV protocol. Generally, it could be noticed that the average end-to-end delay of the AODV protocol is less than both the IDSAODV and the proposed IASAODV protocols due to the doubled waiting time. Starting with 35 nodes the average end-to-end delay of AODV protocol is less than the other protocols. Also the average throughput of the proposed protocol IASAODV is better than both AODV and IDSAODV protocols.

C. SCENARIO 3

Figures 12, 13, 14 and 15 represent the simulation results of the considered protocols. In each Figure, the number of nodes is considered versus normalized routing load, packet delivery ratio, average throughput and average end-to-end delay respectively.

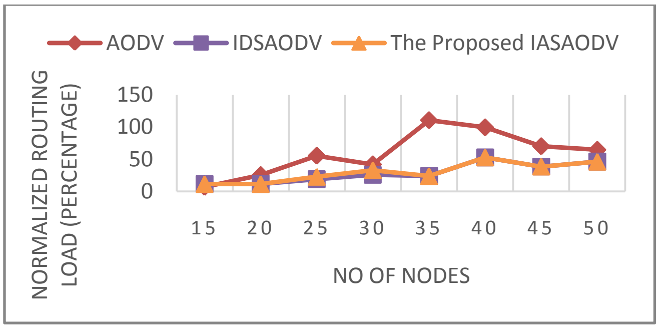

Figure 12: number of nodes vs Normalized Routing Load in case of five black hole nodes attack.

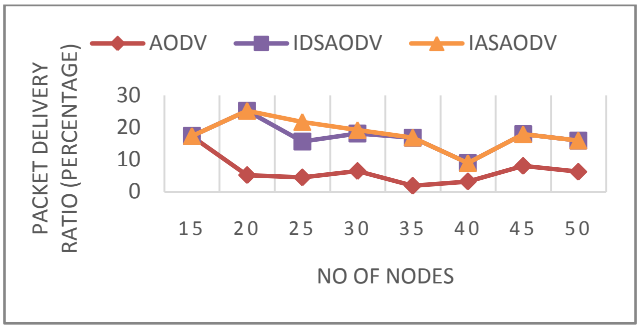

Figure 13: Number of nodes vs Packet Delivery Ratio in case of five black hole nodes attack

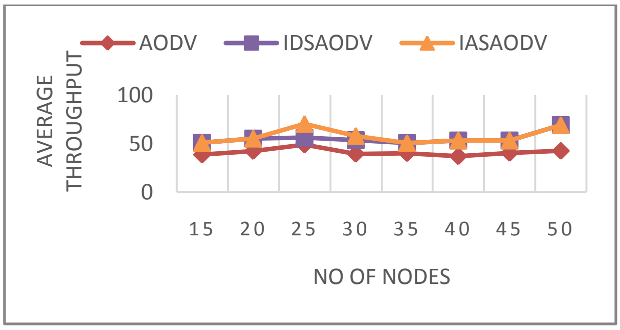

Figure 14: Number of nodes vs Average Throughput in case of five black hole nodes attack

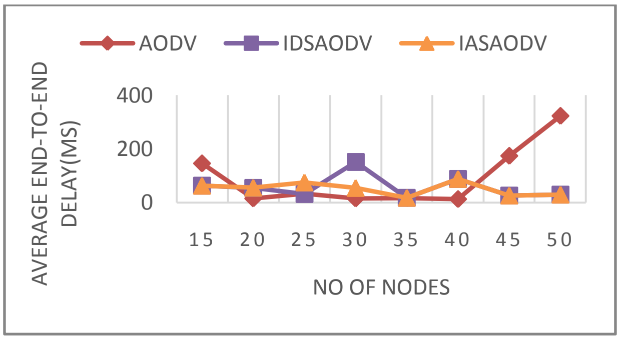

Figure15: Number of nodes vs Average end-to-end delay in case of three black hole nodes attack

From these Figures, It is clear that the proposed that generally the packet delivery ratio and normalized routing load of the proposed protocol is better than both AODV and IDSAODV protocols. Considering average end-to-end delay, the performance of AODV protocol is better than both the other protocols due to the doubled waiting time. As can been seen, the average end-to-end delay of this protocol increased starting with nodes 40 and decreased in the case of both the proposed protocol and IDSAODV protocol.

7. CONCLUSION AND FUTURE WORK

Mobile ad hoc networks (MANETs) are dynamic wireless networks without any infrastructure. These networks are weak against many types of attacks; one of these attacks is the black hole attack. In this attack, a malicious node advertises that it has a freshest or shortest path to specific node to absorb packets to itself. In this paper, a modified AODV routing protocol is introduced to avoid the black hole attack in MANETs. Simulation results using NS-2 simulator depict the packet delivery ratio in the presence of malicious nodes. Three different scenarios for the black hole node(s) are applied; each one is implemented on three protocols AODV, IDSAODV and the proposed IASAODV algorithm. The simulation results showed that the packet delivery ratio (PDR) of the AODV protocol is decreased according to the black hole attack; which means increasing the packet loss of this protocol. The PDR, throughput and NRL of the proposed protocol were better than both AODV and IDSAODV protocols. We can conclude also that as the number of black hole nodes is increased, the PDR of the considered protocols is decreased. As a future work, the effect of other attacks such as wormhole and gray hole on the AODV and other routing protocols used in MANETs will be considered.

8. REFRENCES

[1] Shree.P Vidya and Reena.G Sophia, "A Survey Of Various Routing Protocols In Mobile Ad-Hoc Networks (MANET)," International Journal of Computer Science & Engineering Technology (IJCSET), vol. 3, pp. 224-228, 2012.

[2] Yi Seung, Naldurg Prasad, and Robin Kravets, "Security-Aware Ad hoc Routing for Wireless Networks," University of Illinois at Urbana-Champaign Champaign, IL, USA ©2001 , Technical Report 2001.

[3] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition. New Jersey: Prentice Hall, 2003.

[4] Wu Bing, Chen Jianmin, Wu Jie, and Cardei Mihaela, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Springer, 2006.

[5] E Perkins Charles, M Belding-Royer Elizabeth, and SamirDas, "Ad-Hoc On-Demand Distance Vector (AODV) Routing," in Proceedings of IEEE WMCSA'99, New Orleans, 1999.

[6] Human-centric Computing and Information Sciences, a Springer Open Journal, November 2011 [Online]. Hyperlink "http://www.hcis-journal.com/content/1/1/4"

[7] Tseng Chin-Yang, Balasubramanyam Poornima, and Ko Calvin, "A Specification-based Intrusion Detection System for AODV" in Proceedings of 1st ACM workshop on security of Ad Hoc and sensor networks, California, Davis, 2003, pp. 125-134.

[8] Sitapara Nishant and Sandeep B. Vanjale, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks," in International Conference on Emerging trends in engineering "ICETE-201O" , Jasingpur, 2010.

[9] Himral Lalit, Vig Vishal, and Chand Nagesh, "Preventing AODV Routing Protocol from Black Hole Attack", International Journal of Engineering Science and Technology (IJEST), vol. 3, pp. 3927-3932, 2011.

[10] Yang Su Ming, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Elsevier Computer Communications, vol 34, pp. 107-117, 2011.

[11] Von Mulert Jan, Welch n Ian, and Winston K.G.Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV," Journal of Network and Computer Applications, vol. 35, pp. 1249–1259, 2012.

[12] Khare Shashank, Sharma Manish, Dixit Namrata, and Agrawal Sumit, "Security in Routing Protocol to Avoid Threat of Black Hole Attack in MANET," VSRD International journal of Electrical, Electronics and Communication Engineering, vol. 2 (6), pp. 385-390, 2012.

[13] Ghonge Mangesh and S. U. Nimbhorkar, "Simulation of AODV under Blackhole Attack in MANT," International Journal of Advanced Research in Computer Science and Software Engineering", 2012.

[14] Nabarun Chatterjee and Jyotsna Kumar Mandal, "Detection of Blackhole Behavior using Triangular Encryption in NS2," 1st International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA- 2013), pp. 524-529, 2013.

[15] Sharma Ajay, Babu, Ahirwar Rajesh, and Patil Smita, "Performance Evaluation of AODV under Blackhole attack in MANET using NS2 simulator," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), pp. 79-82, 2012.

[16] Su Mon Bo, Xiao Hannan, Adereti Aderemi, and James A, "A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack," in Third International Symposium on Information Assurance and Security, 2007, pp. 50-55.

[17] The Network Simulator - NS-2 [Online]. Hyperlink "http://www.isi.edu/nsnam/ns/"

[18] K Fall and K Varadhan, “The NS Manual”, the VINT Project, UC Berkeley., 2011.