I. J. Computer Network and Information Security, **2015, 10, 42-49**
Published Online September 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.10.05

A Cross Layer for Detection and Ignoring Black Hole Attack in MANET

Azza Mohammed
Department of Computer science, Djillali Liabes University of Sidi Bel Abbes, Algeria
Email: azza.mohammed.amine@gmail.com

Boukli Hacene Sofiane and Faraoun kamel Mohamed
Department of Computer science, Djillali Liabes University of Sidi Bel Abbes, Algeria

***Abstract*—**MANET Mobile Ad hoc Network are evolved through various characteristics such as shared media, this property make a routing protocols vulnerable. AODV is a reactive routing where each intermediate node cooperates in the process of route discovery. In this case, the node that behaves as malicious exploit the malfunction of specified service. The black hole attack uses the sequence number that is used to select the freshest route and attract all exchanged data packets to destroy them. Many researchers have dealt with this attack and many solutions have been proposed. These solutions target the network layer only. In this paper, we present our approach to counter black hole attack. This approach is entitled CrossAODV and it is based on verification and validation process. The key point of our approach is the use of the inter layer interaction between networks layer and medium access within the distributed coordination function (DCF) to efficiently detect and isolate malicious nodes. During the route discovery, the verification process uses the RTS / CTS frame that contains information about the requested path. The validation process consists of comparing the routing information with the result of verification phase**.** Our Approach have been implemented, simulated and compared to two related studies using the well know NS2 Simulator. The obtained results show the efficacy our proposal in term of packet delivery with a neglected additional delay.

***Index Terms*—**Mobile Ad hoc Networks routing, Blackhole attack, cross layer interaction.

I. INTRODUCTION

The evolution of Mobile wireless Network has affect the field of communication through its advantages such as the absence of physical media and the concept of mobility and the difficulty to use the wiring [1]. Fundamentally mobile wireless networks divided into two modes: the first one is Infrastructure mode uses an access point that manages the access of mobile units to the shared wireless media. The second one is called Ad-hoc(MANET) where there is no infrastructure.

Ad-hoc network is a multi-hop wireless network where all mobile nodes are connected with each other working together to achieve their objective. This kind of networks does not need any centralized administration and there is not condition on its size. Each node can act as a host or as a router or both in the same time.

MANET can be used in special areas such as military area where wired infrastructure may not be suitable for reasons like the high cost or the convenience. It can be rapidly deployed to meet emergency needs and coverage in underdeveloped areas. So there are many applications for ad-hoc wireless networks [2].

MANET are vulnerable. The use of wireless links makes ad hoc network connection susceptible to many kind of attacks from passive listening to active identity spoofing, replying and distortion.

The security objectives for ad hoc networks include confidentiality, integrity, authenticity, non-repudiation, availability.

Establish path between nodes, a routing protocol such as the Adhoc On demand Distance Vector routing protocol (AODV) is needed. AODV is a reactive routing protocol [3] where each node cooperates in the routing process. This makes this protocol susceptible to internal attacks from nodes belonging to the path. An intermediate node can behave as a malicious and it exploits malfunction of AODV.

The Black hole attacks affect mostly reactive protocols and with a great effect on the AODV protocol [4]. It is categorized as denial of service attack in which malicious node answer all request packets by advertising a fresh path to the destination to all neighbors. The black hole attack is an attack active that uses the field of sequence number, which allows choosing the freshest path.

The rest of this paper is organized as follows. First of all we introduce some generalities on ad hoc networks and the AODV routing protocol. This is followed in section 2 by a description of the black hole attack. Section 3 contains a overview of the state in which we present some approach that was already proposed. After that we explain our approach and it evaluation simulation using the well know networks simulation NS2. Finally we conclude and present future perspective.

II. THE AODV ROUTING PROTOCOL

AODV is a reactive routing algorithm designed by Charles E. Perkins and Elizabeth M. Royer [5]. It is suitable for highly dynamic topology networks and is based on the distance vector routing philosophy. Due to node mobility, network topology changes frequently which make the active route out of service and new route should be discovered. AODV uses a sequence number as route freshness indicator [6].

Routes in AODV are discovered on demand. When a node needs a route to a destination, it broadcasts a route request RREQ within the network. Each neighboring node that receives the broadcasted packet must check the freshness of the routing information through sequence number to update its routing table. This request will be forwarded to either the destination node or a node with an active route to the destination. A destination will unicast a response packet RREP to the source trough the preceding node choosing the shortest path with a sequence number greater than or equal to that which was received in the RREQ.

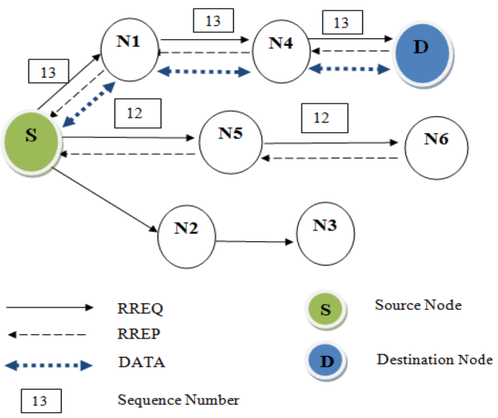

Fig. 1. Process of AODV

After receiving a RREP, a source node begins transmitting data packets to the destination, if later, it receives a RREP containing a sequence number greater or equal, with a smaller metric (number of hops), it will update its routing information to that destination and continue transmitting using the best route.

A route is considered as active as long as there are packets of data transmitted periodically from the source to the destination. When the source stop transmitting data packets, the link will expire and will be deleted from the routing tables of intermediate nodes. If a link fails within an active route, a route repair process is launched by sending a RERR packet to the source. After receiving a RERR, the node source restarts the route discovery process to find a new path [7]. Fig. 1. presents a summary of process of AODV.

A. Medium Acces Layer

The MAC layer is specified in the 802.11 with a variety of functions that support the operation of access in wireless networks. It manages and maintains communication between stations by coordinating access to a shared radio channel and the use of protocols that enhance communication.

The IEEE 802.11 protocol supports two types of access methods. The basic access method is the distributed coordination function (DCF), which is a multiple access mechanism with collision avoidance (CSMA / CA). DCF mode is based on the RTS (ready to send) and CTS (clear to send) mechanism, a node must ensure that the medium is idle before attempting to transmit Fig. 2.

The transmitter sends a control packet RTS to the recipient. All nodes within the communication range of the issuer who received the RTS know that there is a communication will takes place. The destination receives a RTS control packet returns the CTS if it is not itself blocked by NAV (Allocation Vector Network). On receiving the CTS, the sender knows that the medium has been reserved and it can transmit its data [8].

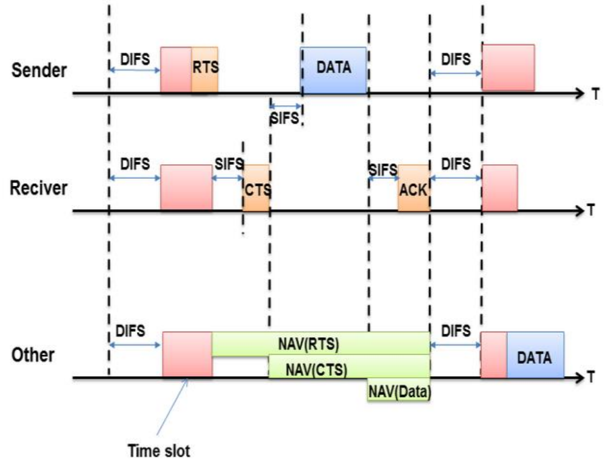

Fig. 2. Distributed Coordination Function (DCF)

B. Black hole Attack

The attacks in MANET are classified into two main categories: passive and active attacks [9]. In passive attacks the malicious node defines an control unauthorized control of some connection to get information on traffic without injecting false information, such as passive listening. In active attacks, the attacker disrupt the normal functioning of the network, it can insert, drop, or modify packets [10]. This represents an actual violation either on network resources or on the transmitted data which disturb the routing process, exhaustion of network resources and breaks the node.

The black hole attack is well known network attack [4]. It is categorized as a dangerous active attack. This attack introduces a serious security issue, in which the attacker injects false routing information in received routing packets to behave as having the best path to destination [10].When the malicious node receives a RREQ packet, it prepares a false RREP packet in which the sequence number field is set to a higher value i.e 2^{32}, and a smaller number of hops [11], if the attacker has succeeded to gain the path, it can intercept all transmitted data packets than drop them [12]. Fig. 3. present a summary of the black hole attack process:

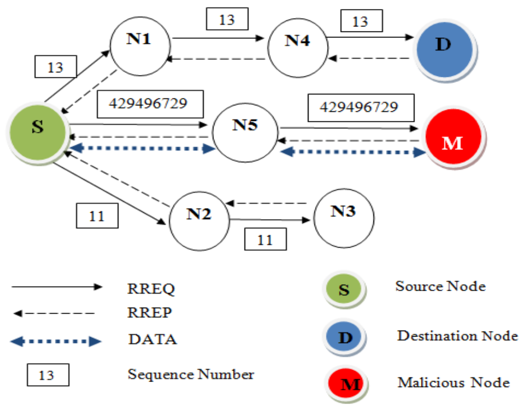

Fig. 3. Black hole Attack

We suppose that the node S wants to send data packets to node D, and M is a malicious node that does not have a valid a route to D. The node M responds directly to the RREQ sent to D, as if it has an active route to the destination using a false RREP packet. In this case, the node M practices a black hole attack in the network. The attacker node can easily ignore and reject any data traffic and conduct a crisis at the network.

III. Related Works

In [13], authors proposed a model based on an audit for Local Intrusion Detection (LID), this is done by the intermediate node between the node sends a RREP and source node. The intermediate node detects an attacker through a new Further RREQ packet (FRREQ) that is sent to the destination across another way. It checks if there is a valid route to the destination. In favorable cases, the destination will responds with a Further RREP packet (FRREP) [13].

A Vani et al [14] proposed a solution to the problem of black hole attack by comparing the sequence number with a prefixed threshold value at each time interval. If the value of received sequence number is higher than the threshold, the node is suspected to be malicious, will be added to the black list, and ignores all reply messages coming through that node.

Preventing AODV Routing Protocol from Black Hole Attack method has been proposed by Lalit Himral et al [15]. The authors proposed a method that verified whether there is a significant difference between the sequence number of the node source and the intermediate node that sent the first RREP. Generally, the first response will be from a malicious node with a destination sequence number very high. The RREP will be stored as the first entry in a Route reply table (RR-table). Then, the source will compare the first received sequence number with destination sequence number, if there is a big difference between them; the node decides that this reply comes from the malicious node, so it will remove the entry from the table.

Subash Chandra Mandhata et al [16] proposed a simple method that does not change the operation of the AODV protocol. It is based on two functions: collection and comparisons. The collection function consists to collect and pre-process RREP packets (Pre_Process_RREP).the second function compares sequence numbers of collected packets, and returns the packet with a higher sequence number if the difference is bigger. The node that sent these packets is suspected to be malicious, in this case, the source broadcasts a packet to alert neighbors containing the identity of the attacker node and all messages received from the malicious node will ignored. Each node should maintain a table of malicious nodes to isolate malicious nodes during communication.

The AODV Protocol have been improved against Black hole Attacks in Nital Mistry et al. [17].They proposed a method that used to store all RREP packets received in a fixed time interval (MOS_WAIT_TIME) in a table (Cmg_RREP_Tab), and then the source node analyzes all the RREPs stored in the table and remove packets with a higher sequence number. The owners of deleted RREP packets are suspected to be malicious and their identity will be stored for the next communication to ignore all packets received from them. The source node selects the RREP with a big sequence number in the table and continues the normal process of AODV.

Yerneni Rajesh et al [18] proposed a method for enhancing the performance of AODV against Black hole Attack. This method is composed of two parts: the phase of suspicion and confirmation. When a node receives multiple RREP, it launches the first phase in which it classes the RREP packets according to their sequence numbers in a descending order. It compares the sequence number of each RREP packets with the average value of the rest. If the sequence number value of a packet is higher and the response time is minim, the owner of the RREP is suspected to be malicious. After detecting suspicious nodes, the source node prepares a new packet MREQ containing a predetermined random number between the source and the destination and sends though all created paths. When the destination receives MREQ, respond with a MREP packet containing the same random number defined by the source. If the source node receives many MREP with the same random number, it trusts the destination and chooses the freshest path.

Harsh Pratap et al [19] proposed a method based on two techniques Reference Broadcast Synchronization (RBS) and relative distance. In the first method, a time threshold that is the duration of packet transmission is fixed. It is used to compare it with transmission duration of each transmitted packet, if duration is greater than the node is malicious. The second technique is the average distance from the reference point that is called threshold point. In the normal case, the distance from the source node to the destination equal to a threshold, if it exceeds the threshold then the source node deduces that the node is malicious.

A dynamic learning system against black hole attack has been introduced by Payal N. Raj et al [20]. It includes a mechanism to verify the received sequence number of RREP packets. When the source node receives a RREP packet it compares the sequence number of the received

RREP to a threshold value. The answering node is believed to be a black hole if its sequence number is greater than the threshold value. The source node adds the suspicious node to its blacklist, and propagates a control message called ‘Alert’ to inform its neighbors. The threshold is the average difference between the destination sequence number in the routing table and the destination sequence number in the received RREP in a period and each time interval this value will be updated. The main advantage of this protocol is that the source node announces the black hole to its neighbor to be ignored or deleted.

IV. Proposed Solution

Our approach consists of two phases, verification and validation of the path through interaction between the routing layer and the medium access layer. If a node seeks a path, it send a RREQ packet at the routing layer, in a layer 802.11 medium access mechanism will be launched based on the DCF. Before sending a RREQ, the transmitter detects if the medium is cleared by creating an RTS packet and sending it to the receiver.

In our approach we have included within this packet request information to get the status of the routing table of the receiver or an intermediate node. The sent back RREP packet contains routing information about the requested path, but before sending this packet a verification process should be done. The verification uses the RTS / CTS frame that contains information about the requested path.

If the node that responds with a RREP is an intermediate node having a path to the destination or is the destination itself, is includes within the CTS frame an information confirming that this node has a valid entry to the destination. After receiving a RREP, the path should be validated by comparing the routing information with the result of verification phase. If the information included in the CTS is true, the path is valid and the transmission can begin. The black hole attacker does not have a routing table and when it receives a RREQ, will responds directly by a RREP having a large sequence number. However, it not includes any verification information by the fact; the receiver node detects the existence of a malicious node.

Pseudo Algorithm of our approach

Declaration

```
 RTS_INF        // request information
 CTS_INF        //response information
 CROSS          //cross_layer information
```

Pseudo Algorithm for Source Node :

BEGIN

```
   Prepare RREQ to send
  Create RTS packets
  RTS_INF == TRUE
/* Request for routing information  added to the RTS  */
  Send RTS to Neighbor Node
  Receive CTS with CTS_INF /*routing information */
  IF (CTS_INF == TRUE) THEN
          CROSS = TRUE
     Else   CROSS=FALSE
  Send RREQ
  Receive RREP
   /*Validation process*/
  IF ((routing information == TRUE) && (CROSS == TRUE)) THEN goto END

     Else
        IF ((routing information==TRUE) && (CROSS == FALSE) ) THEN
              {
                /* Node Source of RREP is a malicious */
                  DROP RREP
                  ADD RREP_Source_ID in malicious Table
                }
```

END

Pseudo Algorithm for Destination Node or Intermediate Node :

BEGIN

```
  Receive RTS
  IF (RTS_INF==TRUE) THEN {
        IF (ROUTING_INF==TRUE) THEN {
            /* cross layer check the table of routing */
          CTS_INF=TRUE
          /* Prepare CTS with routing */
               }
            ELSE {
           /* there is no routing information*/
                  CTS_INF=FALSE
                   }
                                   }
   Send CTS
   Receive RREQ
   Send RREP
```

END

Pseudo Algorithm for Malicious Node :

BEGIN

```
    Receive RTS
    Send CTS without routing information
    Receive RREQ
    Send RREP witch great sequence number
```

END

- Sequence Diagram of our approach

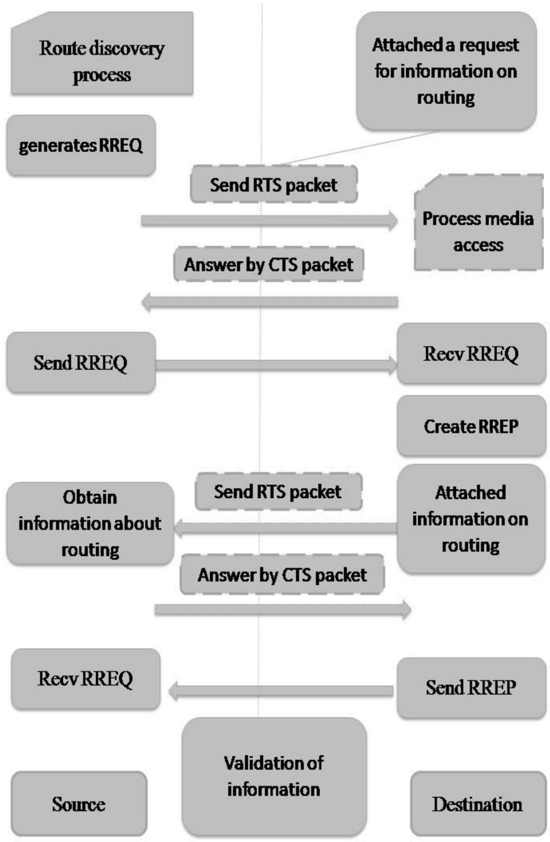

Fig. 4. Sequence Diagram of our approach

V. Performance Evaluation

A. Comparison of Various Solutions to Black hole Attack

The detection techniques using reactive routing protocols introduced in 13, 14, 20 have control rate high against 13, 16, 17 which have a higher delay against another method.

Most of the solutions discussed in particular not showing a better result. Our proposal based on cross layer we minimize the delay and the traffic control (overhead) with we introduce the process of low layer (Distributed Coordination Function) and the comparison is described in the table 1.

B. Simulation Environment

In order to evaluate the performance of our proposal, we conduct a detailed simulation study using Networks simulator ns2.34. Our approach entitled crossAODV under black hole attack was compared to,

- Normal AODV protocol
- AODV protocol under attack
- Method [17] and Method [20]

The Random Waypoint Model (RWP) [21-22] is used as the mobility model of each node. In this model, each node chooses a random destination within the simulation area and it moves to this destination with a random velocity. The simulation scenario is composed of 50 nodes where variation of 10 to 30 nodes communicates and 1 to 7 nodes are malicious.

We set the parameter as shown in following table:

Table. 1. Parameter of simulation

PARAMETER	VALUES
Number of Node	50
The Traffic Types	CBR
Number of Connection	10,20,30
Number of node Blackhole	1..7
The Packet Size	512 Octets
Send Frequency	4 Packets/Second
Speed Maximum	5 M/S
Time of Simulation	200 S
Size of Topology	500 X 500 M

C. Simulation Performance Metrics

- Packet Delivery Ratio (PDR): This parameter represents the percentage of packets delivered to their destinations relative to the packet transmitted in the network. It is calculated as follows:

$$PDR = 100 \times \frac{\sum packets\ receives}{\sum packets\ sends}\ in\% \qquad (1)$$

- The average latency of data packets (End to End Delay): This is the average time required to deliver data packets from the source to the destination successfully, including latency in queues, storage time in buffer.
- Additive costs (overhead): The number of divided packets controls (RREQ, RREP, RERR) the number of received data packets. This criteria illustrates the amount of additives required cost for each received data packet.

D. Discussion

Packet Delivery Ratio (PDR):

Fig.5. illustrates the evolution of the Packet Delivery Ratio (PDR) in situations where the nodes are running: AODV normal and under attack, method [17], method [20] and our proposition cross AODV under attack. This figure shows better performance of PDR in our method comparing to method [17] and method [20]. It displays a decreasing of the PDR metric in protocol AODV under attack against to normal AODV protocol. In Pause time = 0 the degradation of the PDR is 66,31%, this is justified by the fact that more pause frequent change in network topology (nodes are unstable) and malicious nodes have less opportunities to intercept data packets. However the pause time increase, the network topology become more stable which will a negative impact on PDR (pause time = 200 with 90,94% of decreasing comparing to normal AODV protocol with attack).

Table 1. Comparison Of Available Solutions

Method	Technique	Protocol	Node detect	New packet	Update protocol	Overhead	Delay	Number of malicious
[13]	LID	AODV	Intermediate	FRREQ FRREP	No	+++	+++	1..*
[14]	Compare with threshold fix	AODV	Source	-	Yes	++	+	1..*
[15]	Ignorer first RREP	AODV	Source	-	No	+	+	1
[16]	Collected Comparer	AODV	Source	-	No	+	+++	1..*
[17]	Pre-process	AODV	Source	-	Yes	+	+++	1..*
[20]	Compare with threshold dynamic	AODV	Source	ALERT	Yes	++	+	1..*
Our	Cross layer	AODV	Intermediate	-	No	+	+	1..*

This degradation is predictable because the number of transmitted packets is considerably higher than number of received packets. The number of sent packets is important because all data packets are that received by the malicious node are directly ignored. We we observe that the proposed cross AODV improve the PDR to 92% against to protocol AODV under attack.

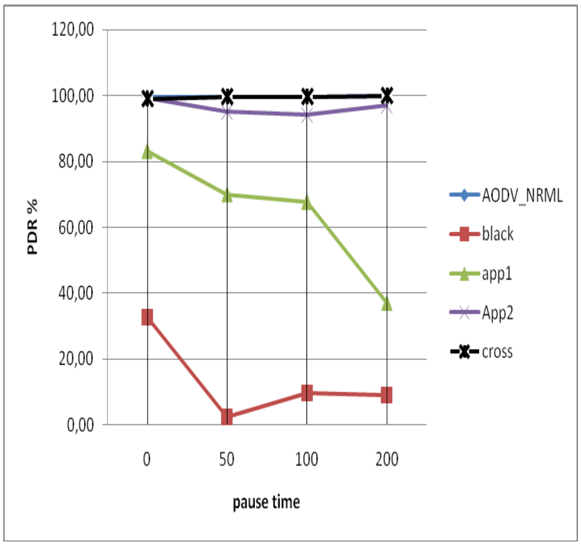

Fig. 5. Effect of pause time in PDR

Communication Overhead:

The Fig. 6. shows an evolution of communication overhead based on Pause time. We note that the protocol AODV under attack generates less communication overhead than the normal AODV protocol. This is explained by the fact that when the malicious node receive the RREQ packets it does not rebroadcast it especially with an increased number of lost data packets in high mobility (pause time = 0), however where the network stabilize (pause time = 200) the number of control packets decreases.

Our approach produces less communication overhead against the method [17] and method [20]. This could be justified the fact that our method does not generate extra control packet for detection, it use the verification and validation process.

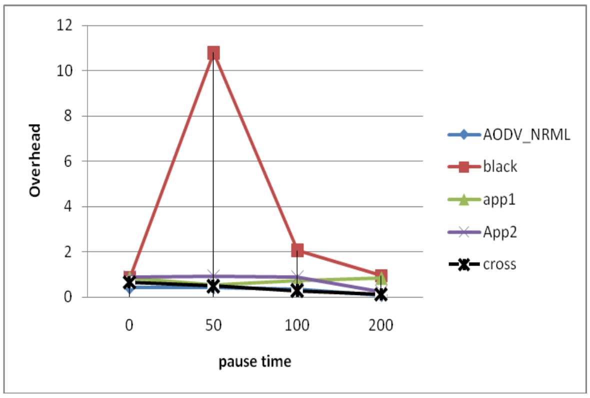

Fig. 6. Effect of pause time in overhead

The Average Latency of Data Packets (Delay):

The Fig. 7. illustrates the decreasing of the average end to end delay according to pause time. In high mobility, and due the high topology changes, nodes are forced to rebuild the invalid paths by discovering new path. However, data packets will be buffered and delayed which increases delay time. When the network stabilizes (pause time = 200) the delay decreases. Our method crossAODV generate higher delay comparing to AODV and AODV under attack. This can argued by the time required by crossAODV to establish a route by avoiding malicious nodes using the verification and validation. However, in normal AODV there is no additional computing.

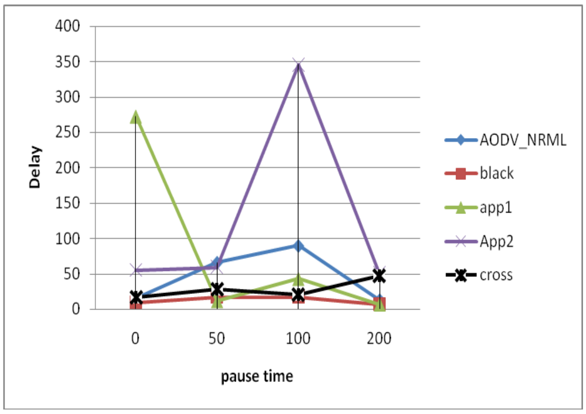

Fig. 7. Effect of the pause time in delay

Influence of Number of Connection:

The Fig. 8. illustrates that when the number of connections increases, the PDR decreases because there is a lot of connections. Many data packets are lost due to overload of network and saturation of queues in normal AODV and crossAODV. In AODV protocol under attack, the PDR increase progressively when the number of connections is increasing because a bigger number of packets are ignored.

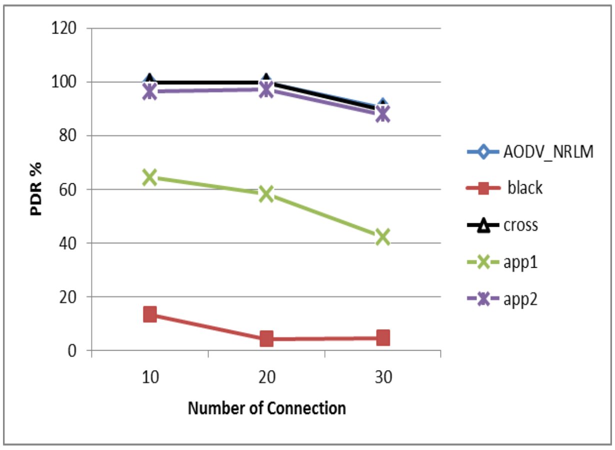

Fig. 8. Effect of number of connection under PDR

Influence of Number of Node Blackhole:

The Fig. 9. illustrates that the PDR is the same as the number of black hole node increase, this conclude that the number of malicious node does not affect in our approach. The degradation of PDR in 30 connections is not due a number black hole, it is because de overload of networks.

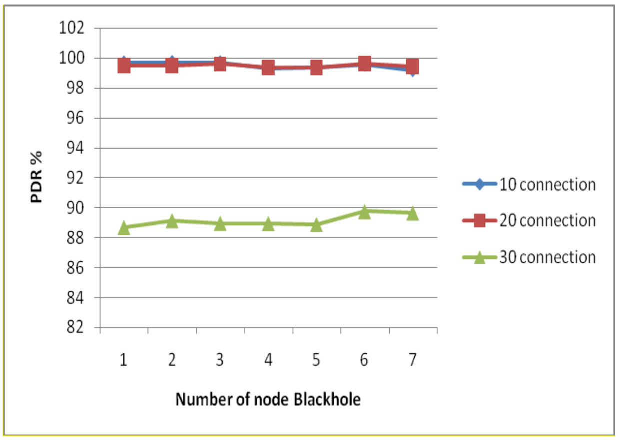

Fig. 9. Effect of number of blackhole

VI. Conclusion

In this paper, we proposed a method called CrossAODV for detection and removal of malicious node that uses the black hole attack in AODV protocol.

This method is based on cooperation between the network layer and medium access layer by exploiting the distributed coordination function. The approach composes of two process: verification and validation. During the route discovery, the verification process uses the RTS / CTS frame that contains information about the requested path. The validation process consists of requesting the same information and comparing the requested routing information with the result of verification phase.

The method was analyzed and compared with related works using different performance parameters such as packet delivery ratio, end to end delay, and overhead. As illustrated in the results, we can easily conclude that the performance of our approach is better compared to related works.

Our solution: CrossAODV increases PDR with neglected increase in average end to end delay and normalized routing overhead, the increases of malicious nodes does not affect our approach.

As perspective, we focus to solving the problem of cooperative of malicious node black hole against AODV.

References

[1] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications. Boston, MA, USA: Auerbach Publications, 1st ed., 2007.

[2] Aarti & Tyagi S. S., "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 252-257, May 2013.

[3] D. Kaur, and N. Kumar, "Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-Hoc Networks", I. J. Computer Network and Information Security, vol. 5, no, 3, pp. 39-46, 2013.

[4] J. Kumar, M. Kulkarni, D. Gupta, "Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, vol. 5, no, 5, pp. 64-72, 2013.

[5] C. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," pp. 90–100, 1999.

[6] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," 2003.

[7] E. Belding-Royer and C. Perkins, "Evolution and future directions of the ad hoc on-demand distance-vector routing protocol," Ad Hoc Networks Journal, vol. 1, no. 1, pp. 125–150, 2003.

[8] Bianchi, G.; Tinnirello, I, "Remarks on IEEE 802.11 DCF performance analysis," Communications Letters, IEEE , vol.9, no.8, pp.765,767, Aug 2005

[9] A. K. Rai, R. R. Tewari and S. K. Upadhyay, "Different types of attacks on integrated manet-internet communication," International Journal of Computer Science and Security (IJCSS) Vol.4, No.3, pp. 265-372, 2010.

[10] P. Rajakumar, V.T Prasanna and A. Pitchaikkannu, "Security attacks and detection schemes in MANET," Electronics and Communication Systems (ICECS), 2014 International Conference on Electronics and Communication Systems (ICECS) , vol., no., pp.1,6, 13-14 Feb. 2014.

[11] M. Roopak, Prof.BVR Reddy, "Blackhole Attack implementation in AODV Routing Protocol" International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 402 ISSN 2229-5518.

[12] M. KS and G. Aghila, "A survey on black hole attacks on aodv protocol in manet," International Journal of Computer Applications, vol. 34, pp. 23–30, November 2011. Published by Foundation of Computer Science, New York, USA.
[13] M. Abdelhaq, S. Serhan, R. Alsaqour, and R. Hassan, "A local intrusion detection routing security over manet network," International Conference on Electrical Engineering and Informatics (ICEEI), pp. 1–6, July 2011.
[14] A.Vani and R. Dr.D.Sreenivasa, "Removal of black hole attack in ad hoc wireless networks to provide confidentiality security service," International Journal of Engineering Science and Technology (IJEST), vol. 3, pp. 2154–2159, March 2011.
[15] H. Lalit, V. Vishal, and N. Chand, "Preventing aodv routing protocol from black hole attack," International Journal of Engineering Science and Technology (IJEST), vol. 3, pp. 3927–3932, May 2011.
[16] D. N. P. Subash Chandra Mandhata, "counter measure to black hole attack on aodv based mobile ad-hoc networks," International Journal of Computer and Communication Technology (IJCCT), vol. 2, no. 6, 2011.
[17] M. Nital, C. J. Devesh, and Z. Mukesh, "Improving aodv protocol against blackhole attacks," Proceedings of the International MultiConference of Engineers and Computer Scientists, vol. 2, march 2010.
[18] R. Yerneni and A. K. Sarje, "Enhancing performance of aodv against black hole attack," in Proceedings of the CUBE International Information Technology Conference, (New York, NY, USA), pp. 857–862, ACM, 2012.
[19] S. Harsh, Pratap and S. Sharma, "Guard against cooperative black hole attack in mobile ad-hoc network," International Journal of Engineering Science and Technology (IJEST), vol. 3, no. 7, pp. 5629–5634, 2011.
[20] P. N. Raj and P. B. Swadas, "Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet," International Journal of Computer Science Issues, vol. abs/0909.2371, 2009.
[21] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," IEEE Transactions on Mobile Computing, vol. 2, pp. 257–269, jul 2003.
[22] S. Talapatra and A. Roy "Mobility based Cluster head selection algorithm for mobile ad-hoc Network" I.J. Computer Network and Information Security, p.p. 42-49, June 2014

Authors' Profiles

AZZA Mohammed received M.Sc in computer science departement from Djilali Liabes University. He is pursuing PhD in Computer Science and Engineering from Djilali Liabes University. He is presently working as Research Scientist in Design and Analysis of Cryptographic Protocols, Network Security and Information Security. He is a life member of EEDIS laboratory.

Boukli Hacene Sofiane Associated Professor at Computer Science Department of the Djillali Liabes University (U.D.L) of Sidi Bel Abbes (Algeria). He received an Engineering degree (first class honors) from U.D.L in 2002, the M.S. degree from Al Al Bayt University at Mafraq (Jordan) in 2005, PhD from U.D.L in 2012 and the habilitation to supervise research (HDR) in 2014. He is a member of the Advanced Networks research team of "Evolutionary Engineering and Distributed Information Systems laboratory" at the U.D.L. His research interests are in networking, including wireless ad-hoc, sensor network, vehicular network and network security.

Faraoun Kamel Mohammed received his M.S. degree in computer science from Djillali Liabes University (UDL) of Sidi-Bel-abbes, Algeria in 2002, and his Ph.D degree in computer science, in 2006, and his Habilitation a Diriger des Recherches (HDR) degree, in 2009, at the same university. His current research areas include computer security systems, cryptography, multimedia communications, genetic algorithms, cellular automata, evolutionary programming and information theory. He is currently Full Professor at computer science department of UDL University. Dr. Faraoun is a member of the Evolutionary Engineering and Distributed Information Systems Laboratory (EEDIS).

How to cite this paper: Azza Mohammed, Boukli Hacene Sofiane, Faraoun kamel Mohamed,"A Cross Layer for Detection and Ignoring Black Hole Attack in MANET", IJCNIS, vol.7, no.10, pp.42-49, 2015.DOI: 10.5815/ijcnis.2015.10.05