Proc. of the Eighth Intl. Conf. on Advances in Computing, Communication and Information Technology - CCIT 2019

ISBN: 978-1-63248-169-6 DOI : 10.15224/978-1-63248-169-6-06

A NEW CROSS LAYER MECHANISM TO SECURE AOMDV AGAINST THE BLACK-HOLE ATTACK

[NAIB Rabiaa, BOUKLI HACENE Sofiane, ALI CHERIF Moussa]

***Abstract*—Mobile ad-hoc networks (MANETs) are a set of mobile nodes that communicate with each other within a common wireless media without the presence of a predefined infrastructure or a central control authority. The absence of preexisting infrastructure is the characteristic that make them ideal for different applications as the military applications. Ad hoc networks rely on routing protocols that are used by nodes to find and maintain routes. AOMDV is one of the well-known multi path routing protocols designed to this kind of networks. AOMDV is vulnerable to different attacks as the black hole attack like any other wireless routing protocol. Black-hole is a network layer attack that deteriorates network performance by capturing data traffic of neighboring nodes and then dropping all received packets. Therefore, securing routing protocols are the most important condition for any secure communication. Numerous solutions were proposed to protect AOMDV against black-hole attacks. A new cross-layer solution for the detection and elimination of the black hole node is presented in this paper. Unlike the proposed solutions, our solution uses the interaction among the network layer and the middle access layer to verify if the intermediate node is a trusted node. To measure the performance of our solution we conducted a detailed simulation study using the well-known NS2 simulator and performance metrics show that our approach performs well and detect perfectly malicious nodes.**

***Keywords*— mobile Ad Hoc networks, AOMDV, black hole attack, cross-layer interaction, performance evaluation.**

I. Introduction

Ad hoc networks contain mobile entities that communicate in a direct way using their wireless communication interfaces. Due to the lack of infrastructure, the mobile units behave as routers that participate in the discovery and maintenance of routes in the network [1]. Various routing protocols have been used to discover routes and rely data packets to the right destination. The key idea of these protocols is to maximize the performance by minimizing packets delivery time, bandwidth usage and power consumption [2]. These protocols can be organized into three different categories [3]: global / proactive for instance [4, 5], on demand / reactive like AODV [6] and hybrid as ZRP [7]. On-demand multipath distance vector (AOMDV) [8] protocol is an expansion to the single path routing Ad hoc On-demand Distance Vector (AODV)[6]. Recall that in MANETs, routing protocols have a tremendous impact. Likewise, each mobile node is considered as a router. Due to the shared communication medium and some protocol design imperfections, AOMDV like all routing protocols is vulnerable to different attacks like black-hole attack[9].This latter is an active attack in which an attacker advertise itself having the shortest path to the destination by sending a fake RREP with the higher sequence number. This malicious node aims to forces its neighbors choosing the announced path for data packets routing. Afterwards, it deletes all received packets. This type of attack can paralyze the network. In this article we describe a new solution to secure the AOMDV routing protocol against black-hole attack. Our approach uses the cross-layer interaction mechanism to detect and isolate the black-hole node.

The remaining of this paper is organized as follows. Section 2, presents the main functionalities of AOMDV. In Section 3, we introduce the black-hole attack. Next, we present some related works. A new cross-layer methodology to detect and isolate the black hole node in Section 5. Section 6 contains the simulation and performance evaluation of our solution compared with AOMDV under black-hole attack using performance metrics. Finally, conclusion and future works are presented.

NAIB Rabiaa
EEDIS Laboratory, University of Sidi Bel Abbes · Department of Computer Science
Sidi Bel Abbes, Algeria

BOUKLI HACENE Sofiane
EEDIS Laboratory, University of Sidi Bel Abbes · Department of Computer Science
Sidi Bel Abbès, Algeria

ALI CHERIF Moussa
University of Sidi Bel Abbes · Department of Computer Science
Sidi Bel Abbès, Algeria

II. Ad hoc On-demand multipath distance vector routing protocol AOMD

Marina and Das in [8] developed a multipath extension to AODV named AOMDV. The main idea behind AOMDV is computing multiple loop-free and link disjoint paths during the route discovery between pair of nodes.

Links disjoint paths means that they do not have any common link in order to avoid that the paths fail dependently.

Proc. of the Eighth Intl. Conf. on Advances in Computing, Communication and Information Technology - CCIT 2019

ISBN: 978-1-63248-169-6 DOI : 10.15224/978-1-63248-169-6-06

If all routes that lead from a source to a destination fail, then a new route discovery process is required.

Recall that in the unipath routing protocol AODV a new route discovery is triggered whenever the single path to a specific destination fails. Thus, AOMDV improve the AODV routing protocol by reducing both route discovery latency and routing overhead.

Fig. 1 shows the route discovery in AOMDV.

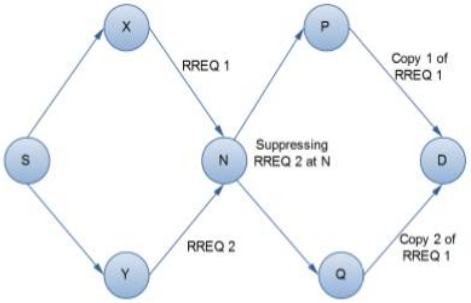

Figure 1. Route Discovery [10]

AOMDV have an important role like other implemented routing protocols in Ad hoc networks. Although, it is vulnerable to different attacks like black-hole attack that will be described in the next section.

III. BLACK-HOLE ATTACK IN AOMDV

Attacks on network layer usually have two purposes: prevent forwarding data packets or modify them [10]. Black-hole is a network layer attack and kind of denial-of-service attack [11] in which, the malicious node after receiving a RREQ packet, it sends immediately a fake REPP packet with a higher sequence number [12] in order to be selected as part of the freshest shortest path to the attacked node.

Therefore, the source node assumes that the malicious node has the freshest route towards destination, it ignores all received RREP packet from the other nodes and starts sending the data packets to the black-hole node. Thus, the malicious node will capture the data packets and drops them.

In *Fig. 2* we assume that the node S wants to send data packets to node D, B is a malicious node. Node B responds directly to the RREQ sent to D by a fake RREP packet with the higher sequence number. After that S choose the RREP of this malicious node. In this case, node B performs a black hole attack in the network by deleting all received data packets.

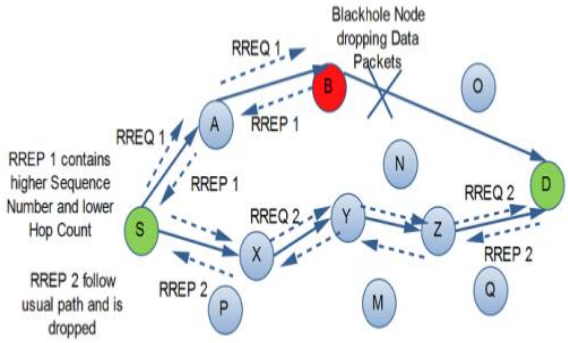

Figure 2. Black-hole Attack [10]

Various methods have been proposed to overcome this problem. Some methods are presented in the next section.

IV. RELATED WORKS

The proposed solutions to secure AOMDV against black-hole attack depends on the mechanisms of detection that can be divided by two categories. In the first category, researchers use cryptographic methods and trust value, however, in the second category; the solution is to improve the routing protocol by modifying the control packets or the route discovery process.

A trust-based multi-path AOMDV routing combined with soft-encryption to secure AOMDV against black-hole attack in ad hoc networks (T-AOMDV) is proposed in [13]. In this approach the message at the source node is segmented into three parts which are encrypted using soft encryption. After that these parts are routed separately through different trust-based multiple paths and then decrypted by the destination node to recover the original message. However, this approach suffers from excessive energy consumption and a huge latency due to the use of cryptographic operations.

In [14] Rani and his working group proposed an improvement of the protocol AOMDV for the detection of black-hole attack.

This improvement consists of modifying the RREQ package by adding a new field named First hop and the RREP packet by adding the originator field, which serves to memorize the identity of the destination node or of the intermediate node who has a fresh route to the destination. Furthermore, each node maintain a legitimacy table that contains two field: The first one named "selection" which indicates how many times a node has been selected during path discovery and the second one named "success" to show how many times the destination received the data packet successfully through the path that contain the node. The characteristic of absence of preexisting infrastructure. A Legitimacy ratio (success /selection) is calculated to identity the malicious node, so, lower the legitimacy ratio, implies higher chances of node being malicious.

An Elliptic Curve Cryptography (ECC) which is a public key cryptographic technique to secure packets against black-hole attack in [15]. In this approach the selection of multi-paths from a source to the destination will be done using the

Proc. of the Eighth Intl. Conf. on Advances in Computing, Communication and Information Technology - CCIT 2019

ISBN: 978-1-63248-169-6 DOI : 10.15224/978-1-63248-169-6-06

AOMDV protocol. Data will be encrypted and decrypted using public and private keys. The source encrypts the packet with the secret key. The destination in turn decrypts the encrypted message to obtain the original data. Thus, the malicious node cannot decrypt the received message because the possibility of retrieve the private key is null.

However, this method requires a lot of computing like encryption, decryption and key generation. Likewise the announcement of the public keys causes an increase of the overload of the network.

Pandikumar and his working groupe apply a measurable technique to mitigate the black-hole nodes in MANETs with the AOMDV protocol [16]. The proposed technique uses an Intrusion Detection System (IDS), which is implemented by modifying the AOMD protocol. The sender must first check the condition of the sequence number whatever it receives a RREP. Therefore, if the sequence number of the fresh RREP is not less than the maximum Sequence number i.e the packet is sent by the attacker with sequence number: 2^{32} , then the source node rejects the new RREP. Otherwise, the source node updates its routing table using the sequence number and the hop count rules.

V. PROPOSED SOLUTION

In our proposed solution we aim to secure the AOMDV routing protocol against black-hole attack in MANET using the cross-layer mechanism. Our method introduces an additional phase “path validation” through the interaction between networks layer and medium access layer to check whether the intermediate node is a trusted node.

In this validation phase we use the XMIT REASON variable with two values: XMIT REASON REPLAY DST and XMIT REASON REPLY IN to indicate the REP initiator. If the intermediate node have a fresh route to the destination node, it must make the variable XMIT_REASON to XMIT_REASON_RREPLY_IN at the MAC layer before it sends the PREP packet. The same process is used for the DST but with the value of XMIT_REASON_REPLY_DST. If the value of the XMIT REASON is different from the two additional values, the source node will have for task:

- Identifies the malicious node.
- Delete the RREP packet.
- Add the blac-khole node to the black list.
- Removes paths that transit through BHN.
- Chooses a different path from the routing table.

Otherwise the intermediate node will become a trusted node.

The following algorithms detailed the behavior of malicious node, source node and destination or intermediate node that have a fresh route.

```
XMIT_REASON_RREP_DST Destination cross-layer information;
XMIT_REASON_RREP_IN Intermediate node cross-layer information;
VI_BH List of black hole nodes;
RP_SRC The sender of RREP;
DST_ADDR The RREP destination address;
SRC The source node;
.....
SEND RREQ;
Receive RREP ;
if DST_ADDR==SRC then
    /* i'm the intended receipient of RREP */
    if FIND(VI_BH,RP_SRC)==TRUE then
        /* The sender of RREP belongs to BH list */
        Remove paths that transit through BHN;
        Delete RREP;
    else
        /* Cross layer check and validation of the path */
        if (XMIT_REASON_ == XMIT_REASON_RREP_DST) or
         (XMIT_REASON_ == XMIT_REASON_RREP_IN) then
            /* The originator of RREP is DST or IN or FW */
            Go to FINISH;
        else
            /* The originator of RREP is Blackhole node */
            Delete RREP;
            ADD RP_SRC to VI_BH;
            Remove paths that transit through BHN;
            Choose a diffrent path from the routing table;
            Delete RREP;
        end
    end
end
FINISH;
```

Algorithm 1. Algorithm for the Source Node.

```
Receive RREQ ;
/*i'm the destination or the intermediate node that have fresh route to
 the destination */
Prepare RREP ;
/*At the medium access layer : in the case of DST*/
XMIT_REASON_ == XMIT_REASON_RREP_DST ;
/*At the medium access layer : in the case of IN*/
XMIT_REASON_ == XMIT_REASON_RREP_DST ;
SEND RREP ;
FINISH;
```

Algorithm 2. Algorithm of the destination or intermediate node that have a fresh route.

```
Receive RREQ ;
/* At meduim acces layer : do nothing */
XMIT_REASON_ ==0 ;
SEND RREP immediately with higher sequence number ;
FINISH;
```

Algorithm 3. Algorithm of the black-hole attacker.

As follows the flowchart that summarizes all steps of the proposed methodology.

Proc. of the Eighth Intl. Conf. on Advances in Computing, Communication and Information Technology - CCIT 2019

ISBN: 978-1-63248-169-6 DOI : 10.15224/978-1-63248-169-6-06

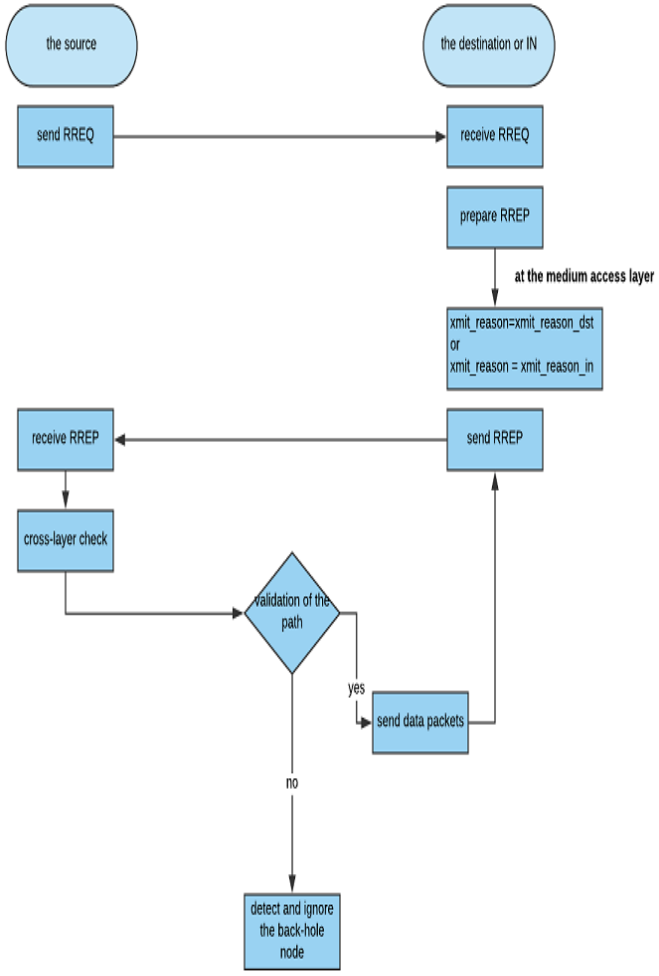

Figure 3. Flowchart of the Proposed Methodology.

VI. PERFORMANCE EVALUATION

A. *Simulation environment*

Our results have been obtained after multiple simulations by varying the number and mobility of communicating nodes (10, 20, 30 and 40).

For the simulations some of parameters have been used. As depict in following table we compare our solution CRAOMDV with normal AOMDV and AOMDV under black-hole attack. In our simulation scenarios the network is composed of 50 mobile nodes with 3 nodes that act as malicious nodes. NS2 [17] simulator was used for simulation and the parameters are summarized in Table 1.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Simulation area (m * m)	1500 * 300
Number of nodes	50
Simulation time (sec)	900
Mobility Model	Random way point
Maximum speed (m/sec)	20
Pause time (sec)	0, 30, 60, 120, 300, 600, 900
Number of communicating nodes	10, 20, 30, 40
Application layer	Constant Bit Rate (CBR)
Packet size	512 bytes
Packet rate	4 packet/second
Routing protocols	AOMDV - BH AOMDV - CRAOMDV
Number of black-hole nodes	3

B. *The simulation performances metrics*

The quantitative metrics chosen for the evaluation of normal AOMDV, AOMDV under black-hole and CRAOMDV are Packet delivery fraction, end to end de-lay and Normalized routing load. These metrics are investigated with different number of connections.

1) ***Packet Delivery Fraction (The rate of delivery of data packets):*** This parameter depicts the percentage of packets delivered to their destinations relative to the packets sent in the network.

$$PDF = \frac{\sum receivedPackets}{\sum generatedPackets} \times 100 \quad (1)$$

2) ***Average end to end delay:*** it defined the average time needed so that the data packets reach the destination successfully. It includes latency in queues and storage time in buffers.

$$AE2ED = \frac{\sum TR_{(i)} - \sum TS_{(i)}}{\sum receivedPackets} \quad (2)$$

With:

$TR_{(i)}$: Instant where the data package is received by the destination.

Proc. of the Eighth Intl. Conf. on Advances in Computing, Communication and Information Technology - CCIT 2019

ISBN: 978-1-63248-169-6 DOI : 10.15224/978-1-63248-169-6-06

$TS_{(i)}$: Instant where the data package is emitted by the source.

3) ***Normalized routing load:*** is the sum of the control packets transmitted per received data packet.

$$NRL = \frac{\sum controlPackets}{\sum receivedPa\,ckets} \quad (3)$$

C. *Discussion and evaluation of results*

1) Packet delivery fraction graphs :

Figure 4. Packet delivery fraction with 10 communicating nodes.

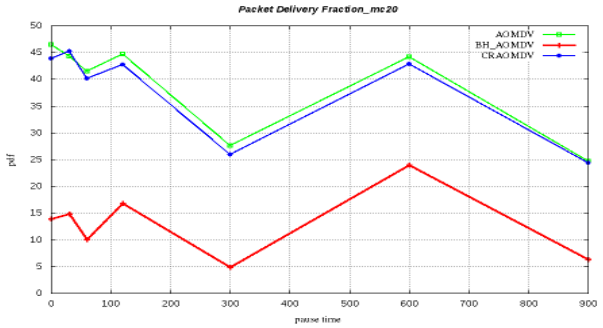

Figure 5. Packet delivery fraction with 20 communicating nodes.

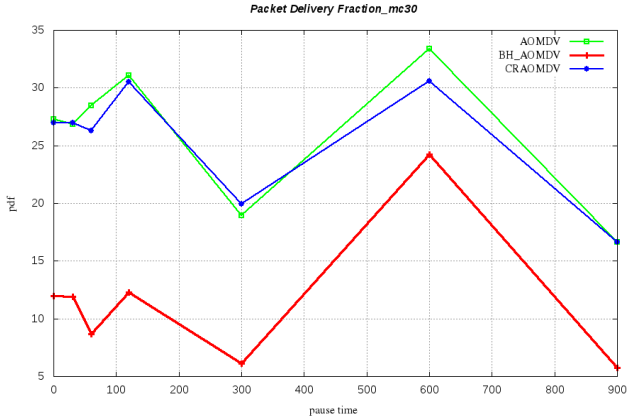

Figure 6. Packet delivery fraction with 30 communicating nodes.

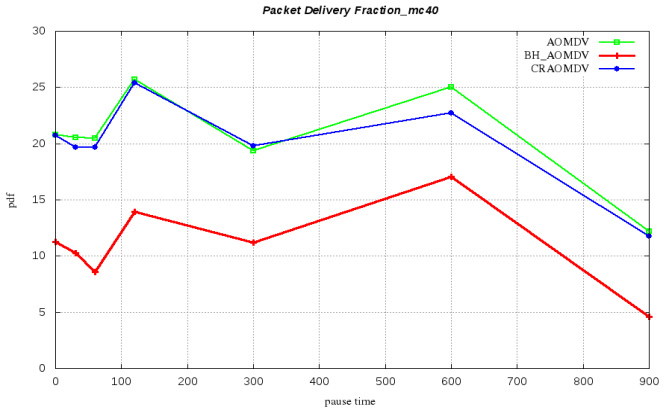

Figure 7. Packet delivery fraction with 10 communicating nodes.

These Figures (*Fig. 4, Fig. 5, Fig. 6 and Fig. 7*) depicts how the number of communicating nodes and pause time influences the packet delivery fraction.

The figures clearly show the inverse correlation between the number of communicating nodes and the PDF, this is due to the network overload and queues saturation in normal AOMDV, BHAOMDV and the CRAOMDV resulting in data loss. In most cases AOMDV, BHAOMDV and CRAOMDV the PDF diminish at once that the mobility decrease and the number of communicating node increase (pt300 and pt900). When the nodes communicate with a low mobility the path between them becomes longer resulting in a higher data loss probability. As can be seen in . *4, Fig. 5, Fig. 6 and Fig. 7* the PDF in BHAOMDV is lower than PDF in normal AOMDV and our approach CRAOMDV because in BHAOMDV, the data packets have been removed by the black-hole nodes.

According to the simulations results, our mechanism "CRAOMDV" perform much better than AOMDV under black-hole attack, and have the PDF almost as normal AOMDV.

2) Average end to end delay graphs:

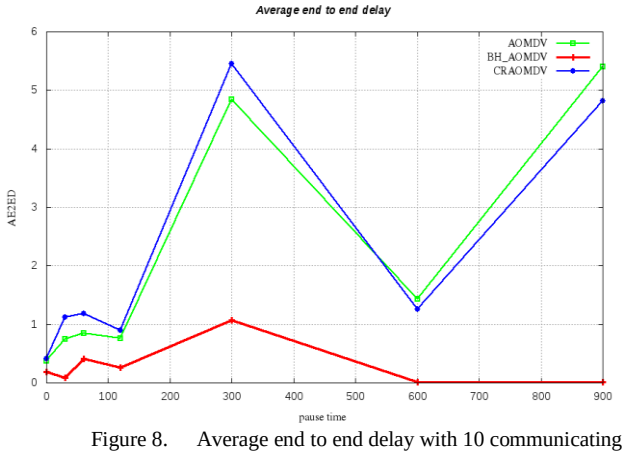

Figure 8. Average end to end delay with 10 communicating nodes.

Proc. of the Eighth Intl. Conf. on Advances in Computing, Communication and Information Technology - CCIT 2019

ISBN: 978-1-63248-169-6 DOI : 10.15224/978-1-63248-169-6-06

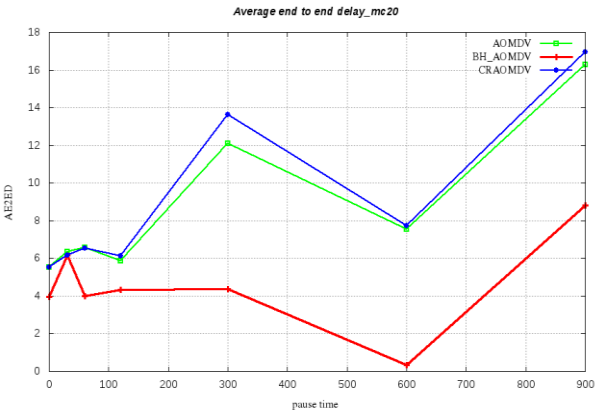

Figure 9. Average end to end delay with 20 communicating nodes.

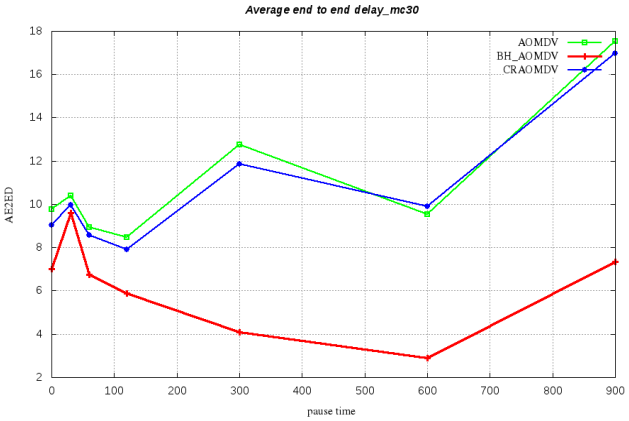

Figure 10. Average end to end delay with 30 communicating nodes.

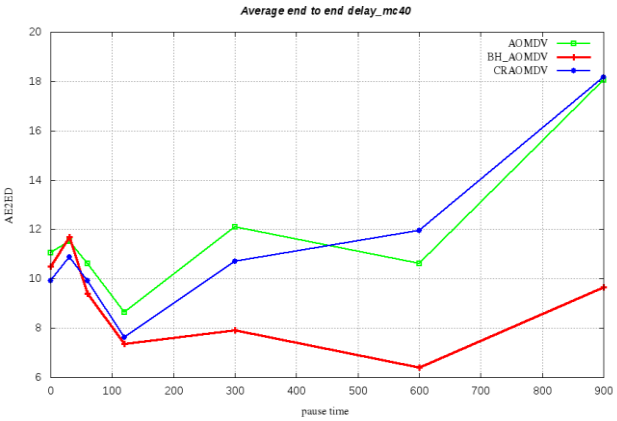

Figure 11. Average end to end delay with 40 communicating nodes.

From the above figures (*Fig. 8, Fig. 9, Fig. 10 and Fig. 11*) we can observe that, as long as the number of communicating nodes increases, the AE2ED increases caused by a high level of network congestion.

The BHAOMDV demonstrates significantly lower delay than AOMDV and CRAOMDV because the data packets were deleted immediately by black-hole nodes without being stored in the buffers or delayed. Our solution CRAOMDV have an A2ED higher as compared to the normal AOMDV protocol with MC10 AND MC20 (10 and 20 sources), this can be explained by the additional time needed by the source node for the verification and validation of the path to the destination. However, CRAOMDV has better delay than AOMDV when the number of node is elevated (30 and 40 sources) and at the same time, the mobility is higher.

3) Normalized routing load graphs:

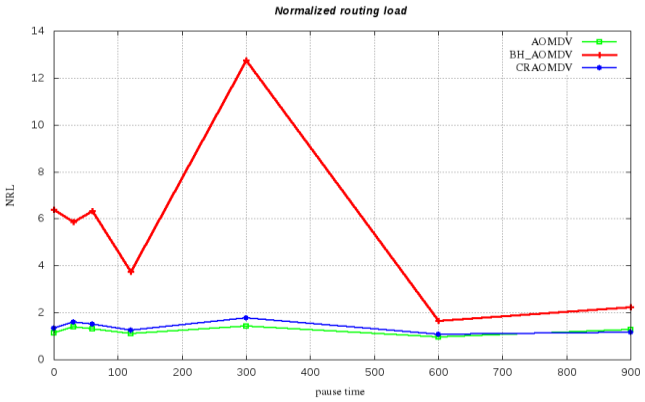

Figure 12. Normalized routing load with 10 communicating nodes.

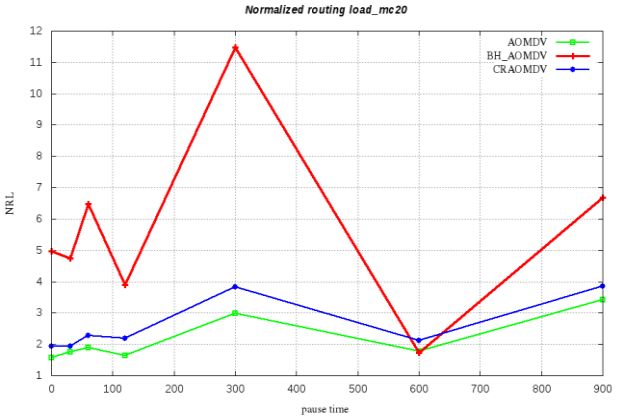

Figure 13. Normalized routing load with 20 communicating nodes.

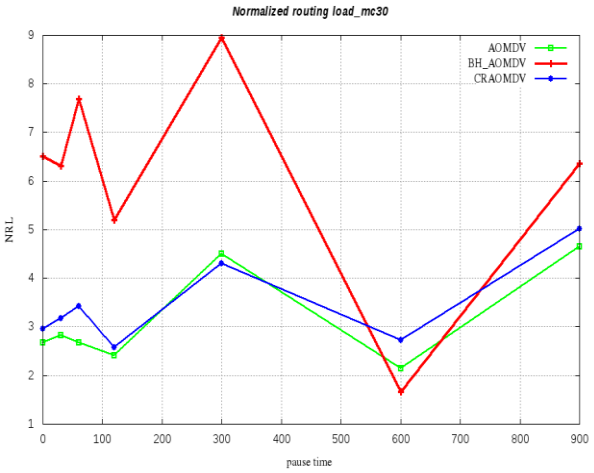

Figure 14. Normalized routing load with 30 communicating nodes.

Proc. of the Eighth Intl. Conf. on Advances in Computing, Communication and Information Technology - CCIT 2019

ISBN: 978-1-63248-169-6 DOI : 10.15224/978-1-63248-169-6-06

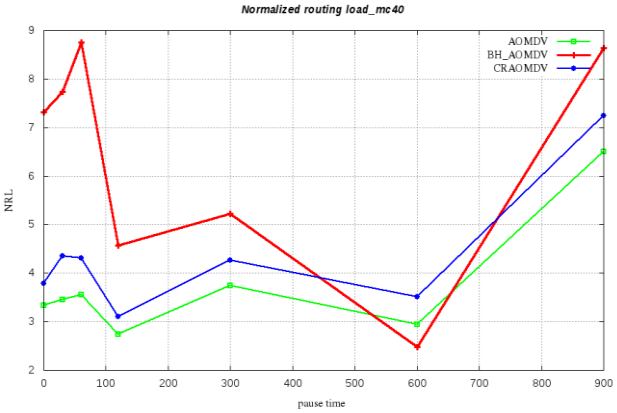

Figure 15. Normalized routing load with 40 communicating nodes.

For the NRL metric, the figures (*Fig. 12, Fig. 13, Fig. 14 and Fig. 15*) illustrate that the value of NRL is higher when the mobility of nodes is bigger (60s, 300s) caused by the unpredictable change in the topology. This frequent change of topology amplifies the number of the control packets. In AOMDV under black-hole attack the sum of packet delivered at the destination is less than the sum of routing packets which decrease the value of NRL as compared as normal AOMDV and CRAOMDV.

From these results it's clear that our solution CRAOMDV is more efficient than AOMDV under black-hole attack because of the higher number of control packet in AOMDV under black-hole attack.

The value of NRL in CRAOMDV is higher as compared to the normal AOMDV, this can be explained by the routing packets send by the source node to find a new path to destination after deleting all paths going through the malicious node.

VII. Conclusion and Future works

In this paper, we present the security issues in MANETs especially the vulnerability of routing protocols to black-hole attack. We analyzed the impact of this attack on AOMDV routing protocol and exposed some of proposed solutions against this type of attack. Likewise, we developed a new cross-layer approach to identify and ignore the malicious nodes thus, find a trusted path to the destination.

Our solution have been simulated using network simulator NS2 and compared to normal AOMDV and AOMDV under black-hole attack.

The simulation performances demonstrate that our solution CRAOMDV perform almost as normal AOMDV and much better than AOMDV under BLACK-HOLE attack by improving the PDF and reduce reducing both route discovery latency and routing overhead. Therefore, prove the effectiveness of our cross-layer solution.

In the continuity of our work, we plan to propose an effective cross-layer security mechanism to eliminate the impact of the cooperative black-attack hole in the AOMDV routing protocol.

References

[1] Joseph Macker. Mobile ad hoc networking (manet): Routing protocol per- formance issues and evaluation considerations. 1999.

[2] Elizabeth M Royer, Chai-Keong Toh, et al. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Commun., 6(2):46–55, 1999.

[3] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2(1):1–22, 2004.

[4] Thomas Clausen and Philippe Jacquet. Optimized link state routing protocol (olsr). Technical report, 2003.

[5] Charles E Perkins and Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In ACM SIGCOMM computer communication review, volume 24, pages 234–244. ACM, 1994.

[6] Charles Perkins, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (aodv) routing. Technical report, 2003.

[7] Nicklas Beijar. Zone routing protocol (zrp). Networking Laboratory, Helsinki University of Technology, Finland, 9:1–12, 2002.

[8] Mahesh K Marina and Samir R Das. On-demand multipath distance vector routing in ad hoc networks. In Network Protocols, 2001. Ninth International Conference on, pages 14–23. IEEE, 2001.

[9] Hongmei Deng, Wei Li, and Dharma P Agrawal. Routing security in wireless ad hoc networks. IEEE Communications magazine, 40(10):70–75, 2002.

[10] Neetika Bhardwaj and Rajdeep Singh. Detection and avoidance of black-hole attack in aomdv protocol in manets. International Journal of Application or Innovation in Engineering & Management (IJAIEM), pages 376–383, 2014.

[11] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, et al. Improving aodv protocol against blackhole attacks. In Proceedings of the International Multi Conference of Engineers and Computer Scientists, volume 2, 2010.

[12] Monika Roopak and BVR Reddy. Blackhole attack implementation in aodv routing protocol. International Journal of Scientific & Engineering Re- search, 4(5):402–406, 2013.

[13] Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S Obai- dat, Ting-Yun Chi, and Sanjay K Dhurandher. Multi-path trust-based secure aomdv routing in ad hoc networks. In Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, pages 1–5. Ieee, 2011.

[14] Jyoti Rani and Naresh Kumar. Improving aomdv protocol for black hole detection in mobile ad hoc network. In Control Computing Communication & Materials (ICCCCM), 2013 International Conference on, pages 1–8. IEEE, 2013.

[15] Sidi-Mohammed Senouci and Guy Pujolle. Minimisation de la consommation d'´energie dans les r´eseaux ad hoc. Annals of Telecommunications, 60(3):500–518, 2005.

[16] T Pandikumar, Biruk Zewdie, and Capt Zinabu Haile. Mitigating black hole attack on manet with aomdv protocol. International Journal of Engineering Science, 12666, 2017.

[17] Teerawat Issariyakul and Ekram Hossain. Introduction to network sim- ulator 2 (ns2). In Introduction to Network Simulator NS2, pages 21–40. Springer, 2012.

Proc. of the Eighth Intl. Conf. on Advances in Computing, Communication and Information Technology - CCIT 2019

ISBN: 978-1-63248-169-6 DOI : 10.15224/978-1-63248-169-6-06

About Author (s):

Rabiaa NAIB received her MS in Computer Science from the Djillali Liabes University (UDL) of Sidi- Bel-abbes, Algeria in 2016. She is pursuing PhD in Computer Science and Engineering from the Djilali Liabes University. Her current research areas include in computer communication (networks), sensor network, vehicular network and network security, computer security and reliability, cryptographic protocols, network security and information security. She is a member of the 'Evolutionary Engineering and Distributed Information Systems' laboratory (EEDIS) and 'Quality of service routing in wireless networks' project.

Moussa Ali cherif has received his Doctorate degree in computer science (2014) and his HDR degree (2016) from Djillali Liabes University (Sidi Bel Abbes Algeria). He is a scientific researcher and member of RSI team (Réseaux ET Sécurité de l'Information) at EEDIS "Evolutionary Engineering and Distributed Information Systems laboratory" at (U.D.L). He is also an Associate Professor of U.D.L. His research interests fall in the general area of Ad-hoc network, wireless sensor networks, acoustic ad-hoc networks, vehicular network and routing based QoS .

Sofiane Boukli Hacene received an Engineering degree (first class honors) from the Djillali Liabes University (U.D.L) of Sidi Bel Abbes (Algeria) in 2002, the M.S. degree from Al Al Bayt University at Mafraq (Jordan) in 2005, PhD and HdR in 2012 and 2014 respectively. He is the Head of "Evolutionary Engineering and Distributed Information Systems laboratory" and "advanced networks and security Research Team" at U.D.L and Associate professor at U.D.L Computer Science Department. He is currently supervising about ten doctoral theses at U.D.L. His research interests are in networking, including wireless ad-hoc, VANETs, WSN, UWN, QoS and security.