Cihan University-Erbil Scientific Journal (CUESJ)

Research Article

Ad Hoc On-demand Distance Vector Inherent Techniques Comparison for Detecting and Eliminating the Black Hole Attack Nodes in Mobile *Ad Hoc* Network

Ghassan A. Qasmarrogy*, Yazen S. Almashhadani

Department of Communication and Computer Engineering, Cihan University, Erbil, Kurdistan Region, Iraq

ABSTRACT

It is important to connect wirelessly a group of moving mobile nodes together in a static or dynamic form, to transfer digital data between them, this form known as a mobile *ad hoc* network. This private network can be used in different essential situations where it depends on each connected mobile node to deliver and pass the data between them, without any fixed access point or router. Unfortunately, there are different types of attacks that can affect these nodes, and steal or corrupt the data inside, one of these attacks called the black hole attack. In this paper, a compared study will be done between two major innovative techniques derived from the *ad hoc* on-demand distance vector routing protocol to avoid the black hole attack; the paper will compare the two techniques in delay, throughput and packet dropping efficacy.

Keywords: Black hole attack, extended data routing information technique, mobile *ad hoc* network, secure *ad hoc* on-demand distance vector routing protocol, trusted *ad hoc* on-demand distance vector

INTRODUCTION

Some scenarios or situation needs a group of moving nodes wirelessly connected together in a static or dynamic infrastructure form; this can be known as mobile *ad hoc* network (MANETs).[1] This form can broadcast or unicast data between each wireless mobile node separately or together. MANET can change its form dynamically depending on the moving nodes speed as shown in Figure 1; therefore, it shows better moving infrastructure to be used for different types of situations such as military, search and rescue, wireless sensor networks, and many more.[2] Where each node can move separately or with its private group to form the new infrastructure without the need of fixed access point or routers. Each node in MANET is responsible for cooperating with other nodes to send and receive the data smoothly using a different type of routing protocols (RPs) that are designed, especially for MANET.

There are three types of RPs for networking transmission operations and routing management, namely, proactive, reactive, and hybrid RPs.[3] Each protocol is depending on the size and the dynamic nature of the topology of MANET.[4] The proactive protocols basically are table driven, meaning. It depends on a specific table that used for routing decisions,[5] while reactive protocols are depending on an on-demand decision where it calculates the path needed for sending the data between the nodes on the same time that they need to transmit the data.[6] Hybrid protocols use both reactive and proactive techniques to deliver the data between the nodes.[7] Figure 2 shows the types of MANETs RPs.

It is essential to secure the data transmitted between the moving nodes to provide maximum security; unfortunately, wireless nodes have many security issues to be attacked.[8] One of these attacks called the black hole attack. In this paper, two major annotative techniques, namely, the trusted *ad hoc* on-demand distance vector (TAODV) RP technique and the extended data routing information (EDRI)-based technique will be compared and evaluated to prevent and detect the black hole attack.

This paper will be organized as follows: In section 1, an explanation will be shown for both black hole attack and it's two preventing techniques; section 3 will demonstrate a comprising between the two techniques; and finally, section 4 will conclude the paper.

Corresponding Author:
Ghassan A. Qasmarrogy, Cihan University, Erbil, Kurdistan Region, Iraq. E-mail: ghassan.qasmarrogy@cihanuniversity.edu.iq

Received: Apr 04, 2019
Accepted: Apr 25, 2019
Published: Jan 20, 2020

DOI: 10.24086/cuesj.v4n1y2020.pp77-81

THE BLACK HOLE ATTACK AND AODV RP

In MANETs, all RPs have security issues, therefore, creating a robust RP to transfer data between the nodes without any security issues is difficult, due to many problems such as share link broadcast wireless channel, node's environment insecurity, the absence of center administration, the limitation of resources, and many more.[9] The essential requirements in any communication system to transfer data are integrity, confidentiality, and availability.[10] These requirements insurance the data will be intact without any eavesdroppers that can intercept or replace the transferred data. There are different types of attacks depending on the involvement of the attacker which can be classified into the passive attack and active attack. Moreover, each one of these attacks can be classified into external and internal attacks.[11]

The Black Hole Attack

One of the active attacks in MANET is the black hole attack, in this attack, one communicating node in the private network, after receiving the RREQ message from the sender node to form a path to the destination and start to transmit the data, replies with a RREP message with a highest sequence number compared to other nodes, forcing the sender to form a path through this node to the destination node, and transmits all the data through this path to that suspicious node, in the end when the suspicious node receives all the data, it will drop it all, without forwarding them to the neighbour nodes,[11] Figure 3 shows the fake RREP from the suspicious node. This attack can be considered a serious threat in any wireless private network because all the transmitted data are dropped without any succeed end to end delivery; therefore, it will increase the threshold of successful packet delivery to 100%.

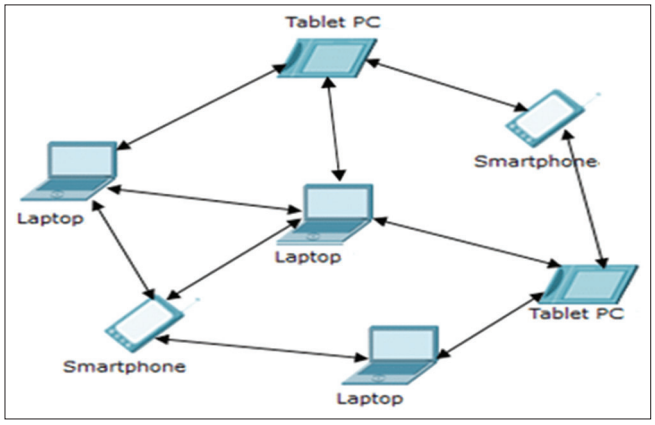

Figure 1: Mobile *ad hoc* network topology

AODV Inherent Black Hole Preventing Techniques

AODV is a reactive RP that starts a discovery route from source to destination when MANET topology changes and the source node want to transfer data, in AODV, each node in MANET stores and uses a routing table, to find the next neighbor node, which has the highest sequence number. In general, before the sender wants to transmit the data, it checks its routing table, therefore if there is a recent route to destination, it will send the data through that path, otherwise it will start a discovery route phase to find more recent route, where the sender will broadcast a request message RREQ to their neighbour nodes and then each node will reply with RREP message, and the highest sequence number node will participate in the path formed.[12]

Trusted AODV routing technique

This technique is built on the original AODV trusted protocol. When new MANET topology is established and a node wants to transmit information to a destination node, it will send a hello message to all other nodes to find the destination, each node after receiving the RREQ message will reply and respond to the sender node with their unique ID; after that, the sender node will be built a neighboring list consist of all nodes around its wireless range, which is stored in the node's memory. This table stores each node's ID in the range, also each node has a trust factor value stored in the table. When the value is small, it means that the node is suspicious, unreliable, and new to the network, and when the value is high, it means that the node is trusted and it was participating in old transmission path

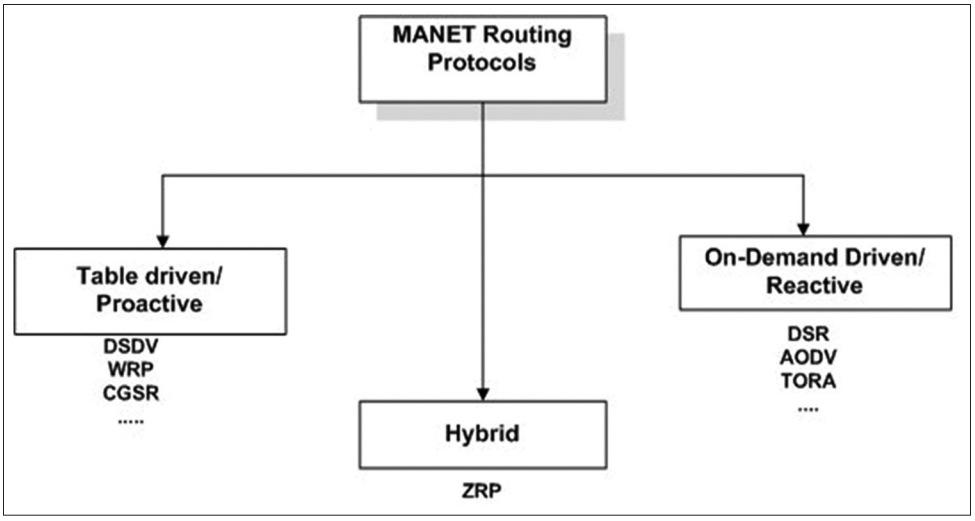

Figure 2: The types of mobile *ad hoc* networks routing protocols

before. Therefore, when the sender node broadcasts the RREQ message, the trusted value function will be used as a feature found in AODV RP to compute the level of trustiness for each node, and when each node receives the RREQ message, they will reply back directly to the sender, so it will be giving a trusting value. After that, when the node involved in a root establishment mechanism, the sender will verify this node by the forward route request RREQ to check its integrity and if the integrity is ok, the trusted value will be increased. After each node stores the trust value factor for intermediate nodes, it would become easier to detect the black hole nodes, so when the sender node will send the RREQ and establishes the path to the destination node, it will make sure that each intermediate node in the path has a higher trust factor, and other nodes with small trust factor will not participate in the future path for a definite time.[13] Figure 4 shows the trusting technique of AODV, where the nodes with higher trusting value are most reliable and with lower trusting value are unreliable.

EDRI technique

The second technique also is an extension from AODV RP; this approach uses a data routing information table (DRI) and an extended data routing information table (EDRI); it also uses a data control packet to detect and discover the suspicious nodes in MANET. Using the EDRI table, each node dynamically updates and stores their current and previous neighbors node's ID, the DRI table including two columns (from and through) and the black hole number (BHN), so when the middle nodes receive a packet from any neighbors' node, it writes 1 in the from column, but when the same node sends the packet to the neighbor note, it writes in the through column 1. When a neighbour node is detected as a black hole the flag of BHN number will be set to 1 and it will be set to 0 when there is no detection. Figure 5 shows the EDRI table.[14]

As known, any suspicious black hole node drops partially or fully all received packets; therefore, control data packets will be sent to check all the middle nodes in the path from source to destination. This packet contains node's id, next node hop NHN, and a random number that are constant for all data packets in that path, this control's data packet cannot be forwarded by a suspicious node. Another data control packet will be also used which can be transmittable by the suspicious node, to check which node did not respond to the previous control data packet. Figure 6 shows the composition of the data control packet.

After receiving all the RREP messages, the sender node will analyze and select the best-secured path to the destination, for transmitting the data packets and detect any suspicious black hole nodes in the path and bandit from future mapping.

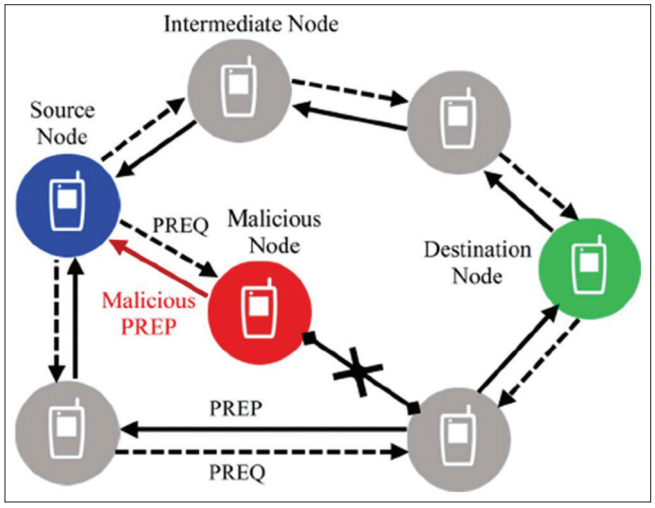

Figure 3: Mobile *ad hoc* network's black hole attack

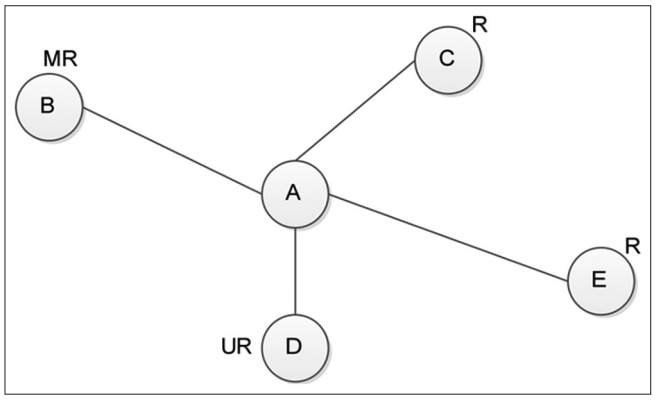

Figure 4: *Ad hoc* on-demand distance vector trusting technique

COMPARISON AND RESULTS

To evaluate the two techniques to prevent the black hole attack and isolate the suspicious nodes from MANET, a scenario was made to simulate the prevention of the attack; the same metric where used to evaluate the two algorithms, packet overhead, throughput, and delay was measured.

When the number of suspicious black hole nodes increases, the end-to-end delay will also be increased, due to the fact of packet dropping, renewal of path formation, and resending of the data message. All of these causes force the sender node to retransmit the packets until it gets acknowledgment from the receiving destination node.

In the trusted AODV (TAODV) technique, when the sender node requests a fresh route, a path to the destination node will be formed, and only the trusted node with higher trusting value will participate in the new path, the trusted nodes

Neighbor node's ID	Data routing information		BHN
	From	Through	
4	0/1	0/1	0/1
2	0/1	0/1	0/1

Figure 5: Example of extended data routing information table

Node_ID	NHN
Random_Number	

Figure 6: The component of the data control packet in extended data routing information technique

number in total are small; therefore, the end-to-end delay will increase. As a result, from the first running transmission, the number of trusted nodes cannot be increased, which causes the sender to use only the available trusted ones, so the delay will not be decreased rapidly overtime. Moreover, when the delay of the message increases, the packet dropping will also increase. Furthermore, the packet overhead will increase and the packet delivery ratio will be decreased due to the previous causes. Figure 7 shows how the number of trusted nodes values increase over multiple transmissions overtime.

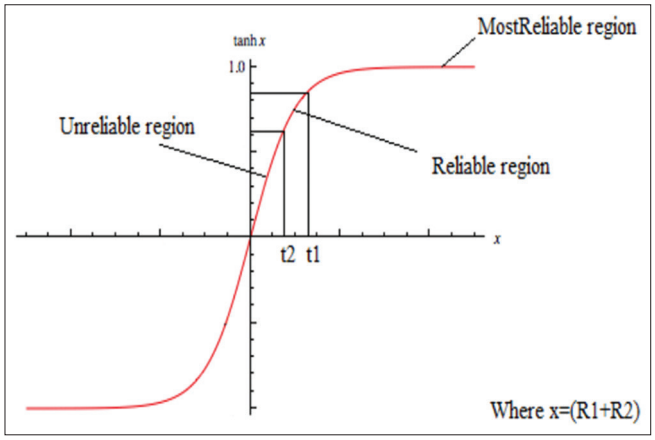

Figure 7: Graph represents the trusted nodes overtime

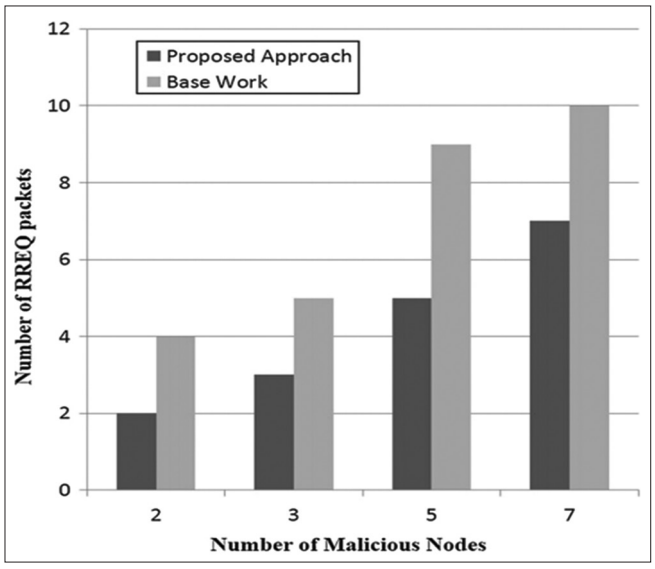

Figure 8: RREQ number evaluation

In EDRI technique, the sender node sends an RREQ packets to generate a safe path, by sending to the neighbor nodes the data control packet, the delay will increase at the beginning of transmission, after that, when all suspicious nodes detected, overtime the delay will be decreased rapidly, due to the fact that all the suspicious nodes were detected in the first running safe path, and no more RREQ packet needs to be broadcasted. Figure 8 shows the decreasing number of RREQ packets overtime.

Moreover, overtime when the number of trusted nodes increases due to EDRI table, the overall delay will be decreased. Moreover, the packet overhead will also be decreased overtime, due to the fact that the sender will reach more trustable nodes so connection packet will not be needed anymore between the neighbor nodes. Figure 9 shows the main comparison of the delay between the two techniques.

The throughput of the network was also compared, in the black hole attack, every single suspicious node sends an RREP to a source node and receives all the data and drops it from that sender, when the number of suspicious node increases, the number of dropping packet increases; therefore, the throughput will decrease. Moreover, when the number of suspicious nodes becomes equal or more than the sender nodes, the throughput will be equal to zero.

In the TAODV technique, the suspicious nodes will not participate in the safe path to the destination, due to the trust value factor, therefore, only the trusted ones will join the safe path, still, the trusted nodes number starting is lower than the normal ones, as a result less throughput and higher packet overhead.

In EDRI technique, all the suspicious nodes will be detected by each sender node in the first run; therefore, the number of

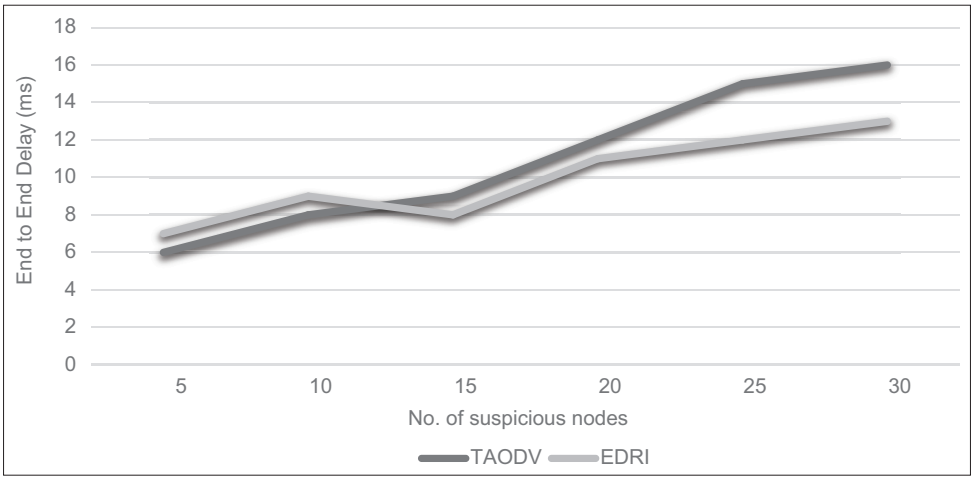

Figure 9: Delay comparison between trusted *ad hoc* on-demand distance vector and extended data routing information

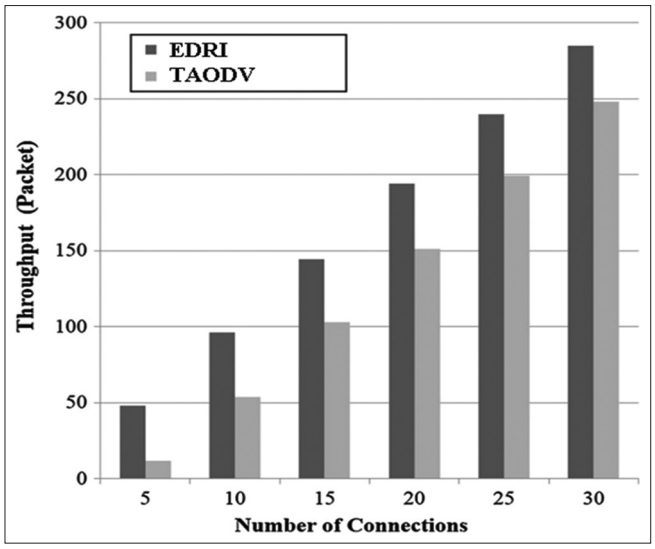

Figure 10: Throughput comparison between trusted *ad hoc* on-demand distance vector and extended data routing information

dropped packets will decrease, throughput will be higher in general, also by time, all the suspicious nodes will be detected, and they will be eliminated, therefore, the throughput will increase through time rapidly. Figure 10 shows the throughput for the two techniques.

CONCLUSION

In this paper, two annotative techniques were compared to detect and eliminate the black hole node attack in MANET, the paper compared three metrics; delay, packet overhead, and throughput.

As a conclusion, the TAODV technique shows a lower delay at the beginning of the transmission, due to the fact that no data control packet was used to detect the suspicious nodes, after that, the delay increases slowly, due to no elimination of suspicious nodes. While in the EDRI technique, the delay higher in the beginning then it decreases rapidly during the time.

In throughput, TAODV shows lower packet delivery compared to EDRI, while EDRI shows better throughput due to the elimination of suspicious nodes overtime, which increases the packet successful delivery.

Finally, both techniques show good delay and throughput to detect the problem of black hole attack nodes, but these techniques work only in one run transmission, new protocols needed to detect multiple runs from the 1st time.

REFERENCES

1. S. B. Sharma and N. Chauhan. "Security Issues and Their Solutions in MANET". IEEE International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), pp. 289-294, 2015.
2. R. Sheikh, M. S. Chande and D. K. Mishra. "Security Issues in MANET: A Review". IEEE 7th International Conference on Wireless and Optical Communications Networks, pp. 1-4, 2010.
3. M. N. Alslaim, H. A. Alaqel and S. S. Zaghloul. "A Comparative Study of MANET Routing Protocols". IEEE 3rd International Conference on E-Technologies and Networks for Development, 2014, pp. 178-182.
4. M. Chitkara and M. W. Ahmad. "Review on MANET: Characteristics, challenges, imperatives and routing protocols". *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 2, pp. 432-437, 2014.
5. R. Shenbagapriya and N. Kumar. "A Survey on Proactive Routing Protocols in MANETs". IEEE 2014 International Conference on Science Engineering and Management Research, pp. 1-7, 2014.
6. D. N. Patel, S. B. Patel, H. R. Kothadiya, P. D. Jethwa and R. H. Jhaveri. "A Survey of Reactive Routing Protocols in MANET". IEEE International Conference on Information Communication and Embedded Systems, pp. 1-6, 2014.
7. R. Dilli and P. C. S. Reddy. "Trade-off between Length of the Hash Code and Performance of Hybrid Routing Protocols in MANETs". IEEE 2nd International Conference on Applied and Theoretical Computing and Communication Technology, pp. 732-735, 2016.
8. A. Dorri, S. R. Kamel and E. Kheirkhah. "Security challenges in mobile ad hoc networks: A survey". *International Journal of Computer Science and Engineering Survey*, vol. 6, no. 1, 15-29, 2015.
9. M. M. Alani. "MANET Security: A Survey". IEEE International Conference on Control System, Computing and Engineering, pp. 559-564, 2014.
10. M. Kuzlu, M. Pipattanasomporn and S. Rahman. "Communication network requirements for major smart grid applications in HAN, NAN and WAN". *Computer Networks*, vol. 67, pp. 74-88, 2014.
11. R. Ranjan, N. K. Singh and A. Singh. "Security Issues of Black Hole Attacks in MANET. IEEE International Conference on Computing". Communication and Automation, pp. 452-457, 2015.
12. M. S. El-Azhari, O. A. Al-Amoudi, M. Woodward and I. Awan. "Performance analysis in AODV Based Protocols for MANETS". IEEE International Conference on Advanced Information Networking and Applications Workshops, pp. 187-192, 2009.
13. M. B. M. Kamel, I. Alameri and A. N. Onaizah. "STAODV: A Secure and Trust Based Approach to Mitigate Black Hole Attack on AODV Based MANET". IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference, pp. 1278-1282, 2017.
14. A. Dorri. "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET". *Wireless Networks*, vol. 23, no. 6, 2017, pp. 1767-1778.