A COMPREHENSIVE SURVEY ON DETECTING BLACK HOLE ATTACK IN MOBILE AD-HOC NETWORK (MANET)

Pascal Maniriho[1], Maurice Ntahobari[2], and Radityo Anggoro[3]
[1, 2, 3] Department of Informatics, Institut Teknologi Sepuluh Nopember
Jl. Teknik Kimia, Gedung Teknik Informatika, Kampus ITS Keputih Sukolilo, Surabaya, Indonesia, 60111
e-mail: manpasco1@gmail.com[1], mntahobari@gmail.com[2], onggo@if.its.ac.id[3]

ABSTRAK

Pergerakan simpul dan kurangnya infrastruktur dalam mobile ad-hoc network (MANET) membuatnya sangat rentan terhadap berbagai serangan. Selain itu, karena fleksibilitas dan kesederhanaan dari MANET, tidak ada standar waktu atau pengaturan izin untuk simpul keluar atau masuk ke dalam jaringan dan setiap node dapat bertindak sebagai klien atau server. Pengamanan komunikasi antar simpul pada MANET merupakan salah satu masalah yang menantang jika dibandingkan dengan jenis jaringan yang lainnya. Pada MANET, serangan dibuat dalam kategori yang berbeda. Black hole merupakan salah satu serangan yang banyak ditangani oleh peneliti dalam beberapa tahun terakhir. Serangan ini terjadi ketika sebuah simpul berbahaya yang disebut dengan black hole menjadi bagian dari jaringan dan mencoba untuk menggunakan kebiasaan buruknya dengan mengirim Route Reply Packets (RREP) palsu untuk bisa menerima Route Request Packet (RREQ). Ketika paket palsu sampai di simpul sumber, simpul sumber akan membalasnya dengan mengirimkan paket data melalui jalur yang telah ditetapkan. Ketika paket sampai di black hole maka akan dibuang sebelum sampai ke simpul tujuan. Dalam makalah ini, kami menyajikan ikhtisar dari berbagai teknik atau metode yang disarankan dalam literatur untuk mendeteksi dan mencegah serangan black hole dalam mobile ad-hoc network. Di samping itu juga menyajikan pengaruh masing–masing pendekatan pada kinerja jaringan.

***Kata Kunci**: — Ad-hoc, Malicious node, MANET, Mobile node, RREQ, RREP, Serangan black hole.*

ABSTRACT

The infrastructure-less nature and mobility of nodes in mobile ad-hoc network (MANET) make it to be very susceptible to various attacks. Besides, owing to its flexibility and simplicity, there is no predefined time or permission set for nodes to leave or join the network and each node can act as a client or server. Nevertheless, securing communication between nodes has become a challenging problem than in the other types of network. Attacks in MANET range into different categories. Black hole attack is one of the attacks that has been addressed by many researchers in the recent years. It does occur when a harmful mobile node called black hole becomes a part of the network and tries to use its malicious behaviors by sending fake route reply packets (RREP) for any received route request packets (RREQ). When these faked packets arrive to the source node, it does reply to them by sending data packet via the established route. Once the packets are received by the black hole node, it drops them before reaching the destination. Hence, preventing the source node from reaching the intended destination. In this paper, we present an overview of a wide range of techniques suggested in the literature for detecting and preventing black hole attacks in mobile ad-hoc network. Additionally, the effect of each approach on the network performance is also presented.

***Keywords**: — Ad-hoc, Black hole attack, Malicious node, MANET, Mobile node, RREQ, RREP.*

I. INTRODUCTION

MOBILE ad-hoc network (MANET) is type of infrastructure-less network where the location and network topology of mobile nodes are dynamically changing [1]. The frequent movement of nodes makes MANET to be a complex distributed system comprises of thousands of mobiles nodes that communicate through wireless links. Each node has the capability to act as router throughout the communication in the network. Since there is no restriction for node to change its location, nodes are more susceptible to many attacks making the security in MANET to be the utmost matter of concern [2]. Routing protocols in MANET are highly prone to security vulnerabilities. A single node or a group of mobiles nodes can be simultaneously compromised. Therein, detecting such malicious behaviors may be even difficult. New network packets can be generated by the compromised nodes and use them to broadcast non-existing links which results in providing incorrect links and flooding other nodes with routing traffic. For some reasons, MANET has got success over a fixed network infrastructure. That is, communication in a fixed wired infrastructure does depend upon the wired backbone Infrastructure and fixed based stations deployed in data centers or elsewhere around the globe. In some cases, setting up such kind of network may be even impossible owing to several reasons such as cost [3][4]. Additionally, factors like radio shadows and natural disasters can make the wired network to be unavailable. Therefore, MANET is widely preferred for various situations such military service, disaster management, rescue operation recovery, hazardous area communication, emergency operations, etc. In military, it allows communication links between soldiers on the battlefield to be established [5]. In rescue areas, it enables a new network to be easily set up in case the existing network infrastructure has been collapsed or destroyed due to disasters such as earthquake or volcanic eruption, so as to get people out of danger.

In addition, this type of network is highly appropriate and preferable in areas where it is awkward to establish a fixed network infrastructure. As the communication between nodes occurs without any fixed infrastructure, the nodes' connectivity is achieved by forwarding network packets across themselves. This connectivity is enhanced by employing some widely adopted routing protocols like "Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector (AODV) and Destination-Sequenced Distance Vector (DSDV)" in each node. Nevertheless, the lack of infrastructure has stimulated snoopers to launch several attacks trying to comprise the security. Black hole attack is one of the attacks encountered in mobile ad hoc network. It occurs when all packets being forwarded to other nodes get absorbed by a malicious node in itself, exactly like a hole which is sucking everything in or somebody sucking a lemonade through a straw. All packets are dropped by malicious node (s). Hence, it results in a route discovery vulnerability preventing packets from reaching the destination.

Similar to any type of communication, the sender (also known as the transmitter) always wishes to transmit data as fast as possible and such data must be kept intact during the transmission [6]. Nonetheless, in MANET, this advantage is taken by attackers who claim to be nearby the destination and start advertising fake shortest path. Besides, due to the limited mobile nodes' battery power, nodes are kept awake till their batteries get down and turn to permanent sleep [7]. Preventing nodes' network resources form being misused is one of the main goals for protecting multi-hope networks. Any effective security architecture should adhere to the requirements such as "confidentiality, integrity, availability, authentication, and non-repudiation" [8].

The remaining part of this paper is structured as follows. A quick learn through of protocols in MANET is given in section II, Section III discusses black hole attacks, various detection and prevention techniques are presented in section IV, Section V provides a recap on the overall effect of each technique with respect to the network performance. Finally, conclusion and the future are provided in the last section.

II. Protocols in MANET

In MANET, if Mobile nodes fall in the same wireless range, they can communicate directly. On the contrary, if the range is different, in order to transfer messages cooperation from other nodes becomes a requirement. Nodes can act as routers or hosts throughout the network. Acting as a router means that they have to control and manage the routing paths which necessitate a routing protocol. Minimizing control overhead, energy consumption and packets loss ratio are the main objectives of routing protocols in MANET. As protocols may be used in different situations, this makes their necessity and complexity to be also different. Basically, considering routing discovery, protocols fall into three groups [9].

1) *On-Demand or Source-initiated protocols:* In this category of routing protocols, routing is performed only when it is necessary. That is, the route discovery process is invoked whenever there is a packet to be sent from source to destination. The route is maintained active until the message reaches the destination. In other words, the route terminates when the communication is no longer needed. DSR and AODV are the examples of protocols in this category.
2) *Proactive or Table-driven protocols:* In contrast to source-initiated protocols, in proactive more than one tables having routing information to every other node have to be maintained by each node. To make sure that the latest updates of the network are maintained, each node keeps on updating its routing table. DSDV is amongst.
3) *Hybrid routing protocols:* Provides a core features from source initiated and table driven protocols. As two categories of protocols recombined, there is a performance enhancement. ZRP is of the routing protocol adopted in this category.

III. Black Hole Attack

One of the denial of service (DOS) attacks in MANET is known as black hole attack [10]. The attack can be launched from the internal or external malicious nodes. In this attack, fake RREP packets are sent by a malicious node (black hole node) to the source node where the route discovery originates from pretending itself to be an intermediate node to the destination or the actual destination node. In this way, data packets would be sent by the source node to the black hole node. As a result, all packets will be absorbed and dropped by the malicious node which will further prevent them from reaching the destination. That is, the source node will no longer be able to communicate with the destination node. It is also worth to mention that malicious node can also forward the sniffed packets to the wrong address. A well labelled diagram illustrating the black hole attack scenario is depicted in Fig. 1 [11].

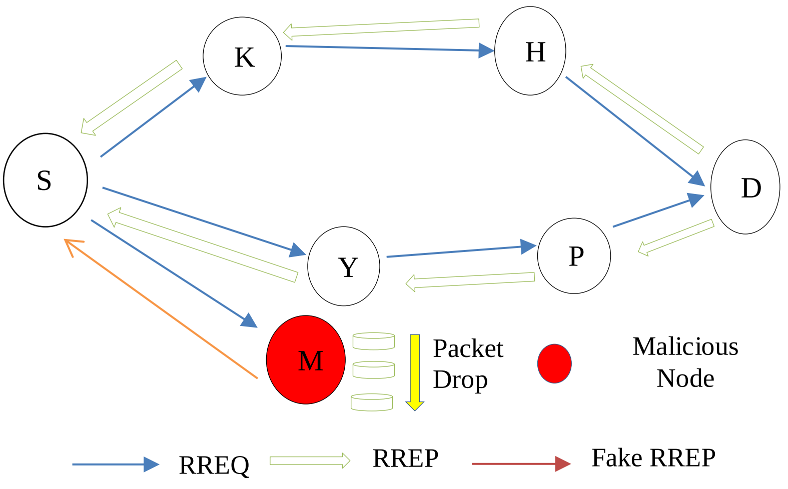

Fig. 1. Black hole attack scenario [11]

In Fig. 1, M is used to denote the malicious node absorbing and dropping all packets from source node (S) preventing them from reaching the destination node (D). Furthermore, two categories of black hole attacks namely, single black hole attack and cooperative black hole attack are elucidated below.

A. *Single black hole attack*

During a single black hole attack, a single harmful node claims to have the shortest and freshest route to the destination by advertising itself. This node always replies to the route request, absorbs and drops data packets from the source node [12]. The scenario can be seen in Fig. 2 [13].

Having the scenario illustrated in Fig. 2, let us now delve on what is exactly happening. First, RREQ packet is broadcasted from node 1 targeting to reach the destination (node 4). Generally, in a normal routing operation, in order to find the possible shortest route to node 4, the RREQ will be rebroadcasted by all neighboring nodes towards node 4. Nevertheless, a malicious node (black hole node) interferes the communication by disobeying the normal routing protocols and transmits RREP packet to node 1 claiming to have the shortest path (also called route) and the highest sequence number to node 4 before any other RREP from normal nodes reaches node 1. Since B's harmful intentions are unknown to 1, the node 1 will start sending data packets to node B, which further absorbs and drops all packets without forwarding them to the destination (node 4).

B. *Cooperative black hole attack*

When more than one single malicious nodes cooperate having the intention to create a black hole attack, the resulting attack is known as cooperative (collaborative) black hole attack. Schematically, Fig. 3 depicts the entire scenario [13].

The example illustrated in Fig. 3 shows the node 1 trying to transmit data to node 4 and two malevolent nodes B1 and B2 working cooperatively. Taking into account the routing procedure of a protocol that does detect a single

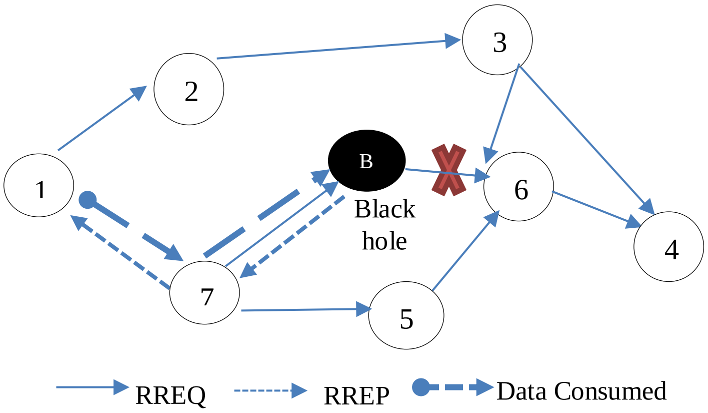

Fig. 2. Single Black hole attack [13]

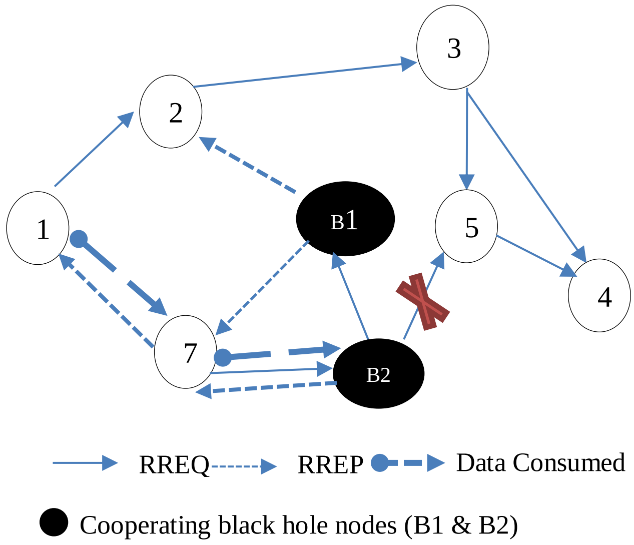

Fig. 3. Cooperative Black hole attack [13]

black hole node, the existence of B1 will be first checked by node 1 through another route such as node 2. Nevertheless, a positive reply will be forwarded to node 2 by B2 since it is cooperating with node B1. Therefore, data will be sent from node 1 to B1 expecting that the route is secure, thereafter, B2 will absorb and drop all packets before being delivered to node 4.

IV. Detection and Prevention Techniques

This section elaborates some of the current techniques for detecting and preventing black hole attacks in MANET.

A. *Nodes' Reliability checking scheme*

In 2013, G. Wahane and S. Lonare [14] suggested a technique for detecting cooperative black hole attack. Overall, their technique works as follows. Two concepts for modifying the existing AODV protocol were first introduced. That is, nodes' reliability checking and maintaining information in the routing table. Three bits of information where two-bits are sent by the nodes that reply to the source node with RREP and one bit of information broadcasted by any mobile node in the network are maintained by every node. The bit 1 is utilized to indicate true while the bit 0 indicates false in the routing table. Besides, nodes' reliability checking is used to check the status of the node whether being trustful or un-trustful based on the next-hoping information available in the routing table, thereafter nodes can be marked as black hole attack or not. Different cases were triggered to examine and identify cooperative black hole nodes in the network.

B. *Trusted AODV*

The work in [15] introduced a new approach that utilizes the trust function to deal with collaborative black hole attacks. The trusted routing behavior is mainly performed based on the trust relationship that exists between nodes. Therein, it is possible to detect and deny any node intending to perform malicious activities throughout the entire network. By considering the defined threshold and the trust on neighbor values, nodes were grouped into three different categories, specifically "unreliable, reliable and most reliable" nodes. Any node having a minimum trust level is said to be unreliable. Typically, when a node joins a network in MANET, its trust relationship level to all its neighboring nodes is relatively low, they treat it as non-trusted node. Reliable node means that its neighbors has received some packets through it.

The reliable node falls between the first and the last category. For Most reliable nodes, the trust level is high. High trust level means that many packets were sent and received successfully by its neighbors through it. The trust value is calculated for each node with respect to its neighbors during the route discovery process. Each node has to maintain a trust table in order to detect any malevolent mobile node. The route going to the most reliable node is always preferred over the one going to reliable node. If it occurs that there is no most reliable node present in the network, the priority is given to reliable node but unreliable node will never be considered to establish route. Re-

TABLE I
DATA ROUTING INFORMATION [16]

Node #	Data Routing Information	
	From	Through
4	0	0
2	1	0

garding the threshold value, to distinguish from the nodes' category mentioned above, different values were defined. That is, a function for estimating the trust value was further suggested. Before transferring data packet, the source node has to check the trust status table to find the suitable and secure route based on the status value and the threshold value. To evaluate the effectiveness of their algorithm, fake packets were sent and all parameters were calculated to identify the status of any nodes.

C. An approach based on Data Routing Information (DRI) table

By using the approach presented by Dorri and Nikdel [16], black holes nodes can be eliminated in the entire network. Each node in the network has to keep information about its neighbors in so called a "data routing information (DRI)" table. To develop the proposed approach, Table I was utilized.

Based on Table I, three main columns are identified, "Node, From, and Through" respectively. The first column is used to indicate the ID of the neighboring node while the remaining columns are used to determine if the node has communicated with the specific node or not. To indicate if data packets from a node that is in "node #" have been received or not by a node, "From" is used while "Through" shows if packets were sent or not by node via a specific node (node in Node column). The proposed algorithm is mainly divided into the following stages.

a) Stage 1: Discovering the freshest path

This stage is employed to discover the best path based on the routing algorithm. Usually, in AODV protocol RREQ packets are first broadcasted whenever a node needs to transfer data to the destination. If a malicious node in the network receives the RREQ packet, it directly creates a RREP having a high sequence number intending to be trusted by the source node as having the best route. This will stimulate the source node to send all data packets to the malicious node. To address this serious problem, the DRI, next and the previous hope's information are included in each RREP after that they are sent to the source node.

b) Stage 2: Path checking

The path which is secure is generated at this stage. The details about the process can be seen in Fig. 4.

c) Stage 3: Malicious node elimination

The objective of this stage is to eliminate all malicious nodes detected on the network. In case a malicious node is detected by the source node, the source creates a packet and the ID of the detected node is appended to the packet which is then broadcasted to the neighboring nodes throughout the network. With this scheme, for any black hole node detected, its information is recorded in the last two columns from Table I as "NULL", hence, no further information will be added by the malevolent nodes in the network.

D. IDS Based Method

In 2011, Su [17] presented an intrusion detection approach for detecting and preventing malicious selective black hole attack in the network. Any node pretending to act as a black hole attack or alternatively as normal is known as a selective black hole attack. In this approach, every node has to execute a mechanism called "Anti-Black Hole Mechanism". By utilizing this mechanism, the node's suspicious value can be estimated based on the abnormal behaviors from both RREQ and RREP. A message has to be broadcasted by the closet IDS whenever the suspicious value surpasses the defined threshold. That is, a notification message will be sent to all nodes in order to collaboratively exclude the detected malicious nodes from the network. The broadcasted message has three fields, the IDS that generates the message, the detected black hole node and the identification time.

After being notified, malicious node will be put to black list. To achieve this, some assumptions were made throughout their experiment. First, Intrusion detection nodes have to be close to each other but in a transition range to allow notification messages to be forwarded between them. Second, all nodes are authenticated to the IDS in order to prevent forging nodes as well as the broadcasted message from being altered or falsified. Third, all network traffic is sniffed by the IDS. Additionally, messages are broadcasted to all nodes in the transition range and to keep track of the malicious nodes, a block table was added to the existing routing table. So, whenever a black hole node

```
Algorithm 1: Steps in checking Path [16]

1  1 Set RREP generate as intermediate Node (IN)
2  Connect to the IN's NHN
3  Ask for its NHN in the path and DRI entries for NHN and IN
4  Check IN if IN is malicious
5  {
6  Mark IN as a black hole node
7  Go to 19
8  }
9  If NHN is trusted or is in the destination
10 {
11 Update DRI table
12 Go to 19
13 }
14 Else
15 {
16 Set NHN as IN
17 Got to 2
18 }
19 Set RREP generator as intermediate node (IN)
20 Connect to the IN 's PHN
21 Ask for its PHN  in the path and DRI entries
22 for PHN and IN
23 {
24 Got to 34
25 }
26 Else
27 {
28 Check if IN  is a malicious node
29 }
30 Mark IN as black hole node
31 Go to 43
32 }
33 }
34 if PHN is trustable or the source
35 {
36 Go to 43
37 }
38 Else
39 {
40 Set PHN as IN
41 Go to 19
42 }
43 If node marked ad malicious
44 {
45 Path is safe. Send data packets
46 }
47 Else
48 {
49 Aware network of malicious node's ID
50 Set Null as DRI entries for malicious
   node
51 Find new path
52 }
```

Fig. 4. Path Checking Algorithm [16]

is identified, it has to be recorded in the block table. The illustration of the proposed IDS nodes’ transition range architecture can be found in [17].

E. An authenticated end-to-end based approach

An approach that deals with simple and cooperative attacks based on end-to-end authentication and acknowledgment was further proposed in 2014, by Baadache and Belmehdi [18]. Since bidirectional packet exchange is required for the proposed solution, wireless links were assumed to be bidirectional. Assuming that M, P, and L are nodes with one node being the successor of the other and having a message (msg) to be transferred from M to L through P. the following points were taken into consideration in order to ensure the effectiveness of the suggested solution.

1. L must generate an acknowledgment confirming that the message has been received
2. P is prevented from sending messages to M trying to impersonate L
3. P cannot alter messages passing via it
4. The attack cannot be led by two nodes that tries to cooperate in end-to-end path

To develop the proposed solution, M and L have to share a common key. All messages being shared between M and L via P are encrypted and decrypted using the key. That is, any message from M going to L via P is first encrypted using the key, thereafter it gets decrypted by C using the common shared key. Besides, a hash function was also utilized to maintain the integrity of messages that pass via a malicious node. According to their experimental results, this approach is able to detect black hole attacks launched in both simple and cooperative way. However, the traffic overhead is slightly generated throughout the network.

F. A dynamic threshold cumulative sum mechanism

To analyze, quantify and detect black hole attacks, in 2016, Panos et al. [19] implemented a novel black hole detection approach that utilizes a “dynamic threshold cumulative sum (CUSUM)” to check the abnormal changes in the normal behavior of the sequence numbers (SQNs) that occurs due to the presence of black hole nodes in the network. In contrast to the other schemes that detect nodes behaving maliciously after discovering unexpected packet drop, this mechanism can highly identify malicious nodes during the first step of the attack. That is, with this approach the intention and the ability of a malicious node to absorb and drop packet is limited. An instance of a detection mechanism that does depend on the audit data is executed by each node in the network. Notice that nodes do not cooperate during the execution of this mechanism. The detection is done by evaluating the SQNs statistical distribution before and after changing. Each time the unlikeness between the two surpasses some predefined threshold, an alarm is directly triggered. The CUSUM value of the threshold can be static or dynamic. During the first phase the CUSUM needs to be trained in order to recognize malicious behavior. Generally, the details about their proposed algorithm including notations can be viewed in [19].

G. Hint Based Probabilistic Approach

The algorithm which is able to identify black hole attacks using probabilistic routing strategy was presented in [20]. In this approach, since nodes can join the transition range at different time intervals, the joining time of each node was considered. Additionally, as nodes may move frequently in the network, this can interrupt the connection, which can cause some communication link breakage. For the sake of discovering nodes’ misbehavior, this breakage time was also considered. The operation of this approach can be summed up as follows. It starts by computing the hint value for all sender’s neighboring nodes. The Hint value is obtained by subtracting the joining time and the time for connection breakage for each particular node. This value is then compared with the threshold. If the hint value is less or equals to the threshold, the status of the node is recorded as “black hole node” otherwise the node’s status is set to” fair node”. After detecting each node’s status, packet will only be transferred to the “fair nodes” while black hole nodes will be discarded from receiving any data packet.

H. Trusted Value AODV Based Scheme

The Authors in [21] introduced the scheme that uses trusted value to discover the best route. That is, with this scheme instead of sending packets via the shortest path, packets are sent via paths that are trusted. Apart from the “trust value”, other parameters such as weight factor and threshold value are taken into consideration. This trusted value is calculated based on each node’s ability to transfer packets as well as its potential to forward RRQ. All packets transferred or received by each node are reordered in order to be used for computing its ability. According to their experimental results, with this approach malicious nodes can be detected and the number packets that are dropped is also considerably decreased. Besides, further information can be found in [21].

TABLE II
COMPARISON BETWEEN BLACK HOLE DETECTION TECHNIQUES

Methods	**Simulator**	**Protocol**	**Type of detection**	**Experimental results**
Nodes’ reliability checking scheme [14]	NS-2	AODV	Cooperative attack detection	It reduces the end-to-end delay and overhead
Trusted hyperbolic[15]	NS-2	AODV	Collaborative attacks detection	The approach enhances the throughput
DRI based approach [16]	NS-2	AODV	Collaborative attacks detection	Processing time and packet overhead are minimized
IDS based method [17]	NS-2	AODV and MAODV	Selective and collaborative attacks detection	The packet loss ratio is improved
An authenticated end-to-end based approach [18]	OPNET Modeler 11.5	AODV and OLSR	Single and cooperative attacks detection	This model achieves good packet delivery ratio for both Protocols. Nonetheless, a traffic overhead is slightly generated throughout the network.
A novel black hole detection mechanism, CUSUM [19]	NS-2	AODV	Single attack detection	Black hole nodes can be detected with a minimal delay and low false positive rate. Besides, it achieves a high detection accuracy and reduces network overhead
Hint based probabilistic routing approach [20]	NS-2	AODV	Single attack detection	The algorithm can decrease the number of dropped packets
Trusted value AODV scheme [21]	OMNeT++	AODV	Single attack detection	Number of dropped packets is considerably decreased
Enhanced modified AODV [22]	NS2-2	AODV	Single and Collaborative attacks detection	This model achieves a high packet delivery ratio. However, it does require more time to identify the malevolent nodes.

I. *Enhanced Modified AODV*

Another technique that prevents collaborative black hole can be found on the work presented by Rana et al. [22] in 2015. The enhancement was done by extending the functionality of the normal AODV protocol. Two additional control packet types are added to the route discovery. From the source node, SRRD_REQ is used while for the destination, SRRD_REP is created. Both Packets control are only kept by the source node and the destination node. Furthermore, the routing table is changed by adding two parameters namely, the "threshold value and the reliability list (RL)". All information about nodes that are trusted is kept in RL while all destination sequence number's average of the reliable nodes is maintained in the threshold field. Based on their experiment, attacks can be detected and prevented throughout the network. The brief overview about all techniques presented in this survey can be viewed in Table II.

V. Conclusion and Future Work

The security vulnerability of mobile nodes in MANET has stimulated many researchers to develop various methods for detecting and preventing black hole attack. Black hole attack is among severe attacks in MANET whereby a malicious node absorbs and drops all data packets from the source node preventing them to be delivered to the destination. The attack can be initiated by a single node or several nodes that work collaboratively to drop data packets and flood other nodes throughout the network. In this paper, routing protocols in Mobile ad hoc network are introduced. Additionally, a comprehensive survey on some of the existing techniques available the literature aiming at detecting and preventing black hole attack is given. In addition, the effect of these techniques on the network performance is also analyzed. By employing these methods, single and cooperative black hole attacks can be detected and prevented in the network. Nevertheless, as it can be seen in Table II, some techniques achieve good detection while decreasing the network performance. Accordingly, we believe that the work presented in this paper will help researchers to easily realize the current status on black hole attack detection techniques. Last but not least, since the security in MANET is still a matter of concern, in our future work we intend to extend this study to various attacks being encountered in MANET.

References

[1] N. Choudhary and L. Tharani, "Preventing black hole attack in AODV using timer-based detection mechanism," *Int. Conf. Signal Process. Commun. Eng. Syst. - Proc. SPACES 2015, Assoc. with IEEE*, pp. 1–4, 2015.

[2] G. Wahane, A. M. Kanthe, and D. Simunic, "Technique for detection of cooperative black hole attack using true-link in Mobile Ad-hoc Networks," *37th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2014 - Proc.*, no. May, pp. 1428–1434, 2014.

[3] R. Prakash, S. Member, and I. C. Society, "Low-Cost Checkpointingl and Failure Recovery in Mobile Computing Systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 7, no. October, pp. 1035–1048, 1996.

[4] A. Harter and A. Hopper, "A Distributed location system for the active office," *IEEE Netw.*, pp. 62–70, 1994.

[5] K. J. Sarma, R. Sharma, and R. Das, "A survey of Black hole attack detection in Manet," *2014 Int. Conf. Issues Challenges Intell. Comput. Tech.*, pp. 202–205, 2014.

[6] F. Stajano and R. Anderson, "The Resurrecting Duckling :Security Issues for Ubiquitous Computing," pp. 22–26, 2003.

[7] G. A. Jacoby, R. Marchany, N. D. Iv, and S. Member, "Battery-Based Intrusion Detection : A First Line of Defense," in *Proceedings of the 2004 IEEE Workshop on Information Assurance*, 2004, no. June, pp. 272–279.

[8] A. Abdelaziz, M. Nafaa, and G. Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks," in *UKSim 15th International Conference on Computer Modelling and Simulation Survey*, 2013.

[9] S. N. Ferdous and S. Hossain, "Randomized Energy-Based AODV Protocol For Wireless Ad-Hoc Network," in *iCEEiCT*, 2016, pp. 1–5.

[10] A. M. Kanthe, D. Simunic, and M. Djurek, "Denial of Service (DoS) Attacks in Green Mobile Ad – hoc Networks," in *MIPRO*, 2012, pp. 675–680.

[11] S. R. Deshmukh, P. N. Chatur, and N. B. Bhople, "AODV-Based Secure Routing Against Blackhole Attack in MANET," pp. 1960–1964, 2016.

[12] R. Kashyap, "Prevention of Black Hole Attack in MANET," *Int. J. Comput. Eng. Res. Trends*, vol. 351, no. 5, pp. 2349–7084, 2015.

[13] B. Singh, D. Srikanth, and S. C. . Kumar, "Mitigating effects of Black hole Attack in Mobile Ad-hoc Networks : Military Perspective," in *IEEE International Conference on Engineering and Technology (ICETECH)*, 2016, no. March.

[14] G. Wahane and S. Lonare, "Technique for detection of cooperative black hole attack in MANET," *2013 4th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT*, 2013.

[15] S. Singh, A. Mishra, and U. Singh, "Detecting and avoiding of black hole attack on MANET using trusted AODV Routing Algorithm," in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, vol. 87, pp. 5–10.

[16] A. Dorri and H. Nikdel, "A New Approach for Detecting and Eliminating Cooperative Black hole Nodes in MANET," in *IKT2015 7th International Conference on Information and Knowledge Technology*, 2015, pp. 1–12.

[17] M.-Y. Su, "Preventi on of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," *Comput. Commun.*, vol. 34, no. 1, pp. 107–117, 2011.

[18] A. Baadache and A. Belmehdi, "Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks," *Comput. Networks*, vol. 73, pp. 173–184, 2014.

[19] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, Quantifying, and Detecting the Blackhole attack in Infrastructure-less Networks," *Comput. Networks*, vol. 113, pp. 94–110, 2016.

[20] Pooja and R. K. Chauhan, "An Assessmnet Based Approach To Detect Black Hole Attack In MANET," in *International Conference on Computing, Communication and Automation (ICCCA)*, 2015, pp. 552–557.

[21] R. K. Bar, J. K. Mandal, and M. M. Singh, "QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack," in *International Conference on Computational Intelligence: Modeling Techniques and Applications CIMTA)*, 2013, vol. 10, pp. 530–537.

[22] A. Rana, V. Rana, and S. Gupta, "EMAODV: Technique to Prevent Collaborative Attacks in MANETs," *Procedia Comput. Sci.*, vol. 70, pp. 137–145, 2015.