AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Black Hole Malicious Behaviour via Different Detection Methods

[1]Layth A. Al dulaimi, [2]R. Badlishah Ahmad, [3]L.A. Hassnawi, [4]Israa Sh. Ahmed

[1,4]Research Student, School of Computer and Communication Engineering, University Malaysia Perlis (UniMap), Malaysia.
[2]Professor Ir. Dr., Dean of School of Computer and Communication Engineering, University Malaysia Perlis (UniMap), Malaysia.
[3]Senior lecture, Al-Mustaqbal University College, Ministry of Higher Education, Iraq.

Address For Correspondence:
Layth A. Al dulaimi, Research Student, School of Computer and Communication Engineering, University Malaysia Perlis (UniMap), Malaysia.

ARTICLE INFO

Article history:
Received 11 September 2016
Accepted 10 November 2016
Published 28 November 2016

Keywords:
Mobile ad hoc networks, Routing protocols, Single black hole attack, Collaborativeblack hole attack, Black hole malicious behaviors.

ABSTRACT

A Mobile Ad-Hoc Network (MANET) is an autonomous wireless networking system consisting of independent nodes that move and dynamically change network connectivity. Mobile Ad hoc wireless networks eliminate the constraints of infrastructure and enable devices to create and join networks anytime, anywhere. The lack of infrastructure and nodes mobility in mobile ad hoc networks makes this type of network vulnerable to different types of network attacks. One of the most import types is black hole attack. Black hole attack is the simple but effective type that is based on the insertion of a malicious node having the capacity to take the identity of valid nodes on an ad hoc network. This insertion leads to disturbances in the network and that due to the participation of all the nodes in the routing. Since a malicious node gives false information of having shortest route to the destination node so as to g*et al*l data packets and drops it. In MANET it's hard to detect behavior anomalies especially to determine the authenticity of messages of applications including routing protocols because changes occur very frequently. No central authorities or infrastructures remain in place for key management or for other proactive or preventive security measures. The strict performance management including latency that is inherent in any security protocol is not possible because performance cannot be guaranteed over a MANET. In this paper, we survey different classifications of black-hole battling strategies which are pernicious conduct classification and we discuss the state-of-the-art of different routing methods as well as the attributes of every strategy and its impact on system execution. Moreover, we compare and analyze the existing solutions and its effects on network performance for different performance metric and for different network performance.

INTRODUCTION

Wireless network is an important technology that allows users to access services and information electronically, regardless of their geographical position. Mobile Ad hoc network is one of the most important types of wireless networks. Mobile Ad-Hoc Network (MANET) is an autonomous wireless networking system consisting of independent nodes that move and dynamically change network connectivity (Verma *et al*. 2008; Mistry *et al*. 2009). In MANET, the nodes are free to move randomly, thus the network's wireless topology may change rapidly and unpredictably. Mobile Ad hoc wireless networks eliminate the constraints of infrastructure and enable devices to create and join networks anytime, anywhere—for virtually any application since an Ad hoc wireless network is self-organizing, self-configuring and adaptive (Mbarushimana and Shahrabi, 2007; Chatterjee and Routray, 2011) . Any node in an Ad-hoc network can function as source, destination, or intermediate node between any source and the destination (Verma *et al*. 2008; Nadeem and Howarth, 2013) .

Open Access Journal
Published BY AENSI Publication
© 2016 AENSI Publisher All rights reserved
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

To Cite This Article: Layth A. Al dulaimi, R. Badlishah Ahmad, L.A. Hassnawi, Israa Sh. Ahmed., Black Hole Malicious Behaviour via Different Detection Methods. ***Aust. J. Basic & Appl. Sci.,*** *10(16): 149-160, 2016*

The random nature of ad hoc mobility without any fixed infrastructure, broadcast nature of wireless channels, and collaborative multihop communications among mobile nodes of mobile ad hoc networks increase the vulnerabilities (Lo and Liu, 2013; Pani and Mishra, 2014).

Penetrations can be classified based on attacker behavior into passive or active. A passive penetration is interested in the significant information regardless of cutting routing process by spying on the traffic. While active penetration presents more serious attack as illegitimate access to the network by intersecting routing process to reduce the performance of the network. Examples of possible active security penetrations in MANET: rushing attacks, wormhole threats, black hole attacks (Umang *et al*. 2010; Jamali, 2015). Byzantine attack (Thanvi *et al*. 2015), attacks on routing table access as well-poisoning route caches, gray hole attack (Tseng *et al*. 2011, Yang *et al*. 2012; Nandakumar and Nirmala, 2016), and distributed denial of service threats (Wu *et al*. 2007; Amutha and Kannan Balasubramanian, 2015). Black hole attack is a serious security attack as it intentionally able to redirect the flow of information away from the proposed destination, as an aggressive node acts to possess the ideal path to destination node and adapts denial of service behavior by killing data packets (Marti *et al*. 2000; Yang *et al*. 2012) or forwards data packets to undesired destination (Marti *et al*. 2000; Tseng *et al*. 2011; Kamatchi and Mukesh, 2013).

This main objective of this paper is to reviews the effects of black hole attack as well as the significant approaches to decrease these effects in MANET by organizing them under categories. Moreover, exhibiting the characteristics of each approach and its influence on network performance.

The random mobility patterns of mobile nodes of a MANET make it hard to detect behavior anomalies especially to determine the authenticity of messages of applications including routing protocols because changes occur very frequently. No central authorities or infrastructures remain in place for key management or for other proactive or preventive security measures. The strict performance management including latency that is inherent in any security protocol is not possible because performance cannot be guaranteed over a MANET.

The main contributions of this paper are demonstrating the effects of black hole attack and presenting the significant approaches to decreases these effects in MANET as well as comparing and analyzing the influences of main characteristics of each approach on network performance.

Black hole attack:

One of the most important attacks in MANET that affect the network security is black hole attack. Black hole attack is classified based on the way of attack into simple and cooperative. Normally a simple or also known as ordinary black hole attack likely occurs in MANET when a bad-intentioned node (malicious node) tampers packet stream (Jamali, 2015), and exploits routing protocol to answer the request from source node RREQ with a fake reply packet RREP pretending to own the ideal path to the goal node supported by most high sequence value as an evidence (Patel and Trivedi, 2014). And consequently bad–intention node (black hole node) blocks data packets from being delivered to the goal node or even being forwarded to neighboring nodes (Suryawanshi and Tamhankar, 2012). Figure 1 depicts the simple black hole behavior.

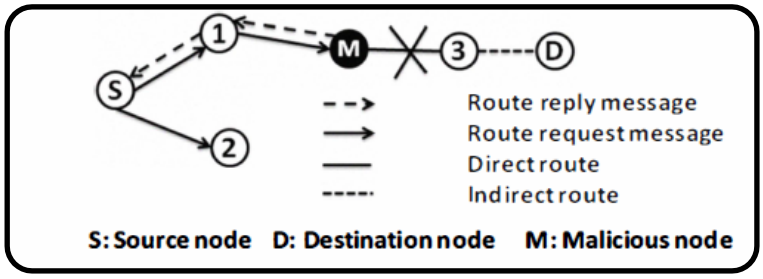


Fig. 1: simple black hole attacking

On the other hand, in the cooperative black hole a group of nodes, at least two adjoining bad-intentioned nodes aggressively collaborate to stop data packets from reaching to its legitimate destination. This attack is more threatening than the simple black hole attack due to the nature of effortless attack execution and difficulty of being revealed by other participating nodes in the network (Lo and Liu, 2013). The cooperative attack is simply accomplished when a black hole-intentioned node is the first among other neighbors of the source node .This node received a RREQ packet from the source node to answer with fake RREP packet concerning best route to the destination. Consequently, the source node begins to push data to the black hole-intentioned node, which is, in turn, pass data packets to the next black hole teammate either who will imprison the data packets or participate with the black hole teammate to swallow the data rather than passing it to the legitimate destination. Figure 2 shows a sample to cooperative black hole node in which S and D denoted to source node and destination node sequentially while B1 and B2 denoted to cooperative black hole attack nodes.

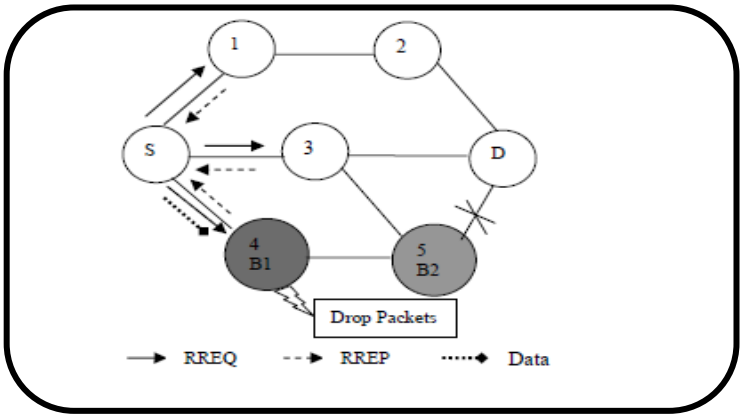


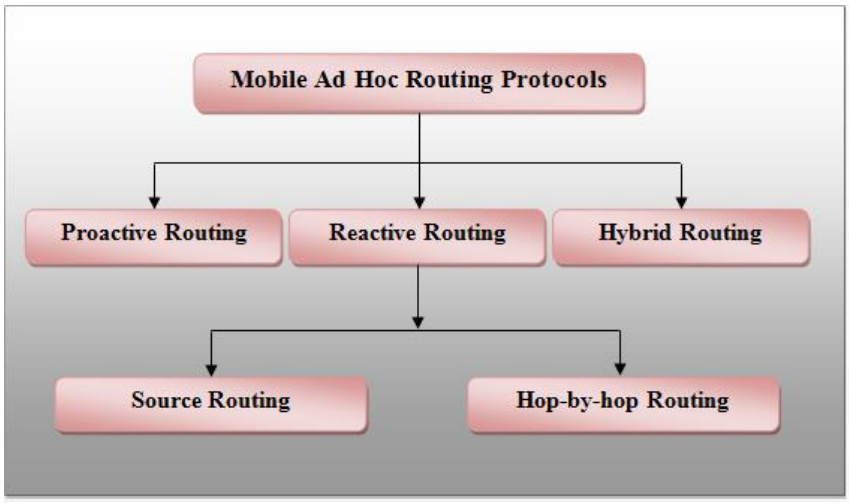
Fig. 2: cooperative black hole attacking

Based on ability of black hole attacking nodes in both types simple and collaborative to tamper routing information it is obvious that black hole attack impacts on network layer (Chandra and Thakur, 2015) and it is considered as sort of denial of service threats that damages transmission of the network layer (Salem and Hamamreh, 2016). Successful schemes are suggested in an attempt to reveal and block simple black hole threat. However, the efficient detection of cooperative black hole attack is still invincible to schemes used for detecting simple black hole that motivates researchers to suggest more schemes for that purpose. It is worth mentioning that black hole attack does not pose a threat to communications security in MANET only but also in Vehicular Ad Hoc Network (VANET) (Tripathi and Venkaeswari, 2015)and Wireless Mesh Networks (WMNs) (Navamani and Yogesh, 2015). In the literature review section, some of the most common schemes to detect both types of black hole attack are reviewed and compared.

Routing protocols in MANET:

The highly dynamic nature of mobile ad hoc networks results in frequent changes and unpredictability in network topologies, adding difficulty and complexity to routing among the mobile nodes within the network. These added challenges, coupled with the critical importance of routing protocols in establishing communications among mobile nodes, make the routing as one of the most important gates exploits by the aggressive node(s) to attack the network. There are different criteria for classifying routing protocols for wireless Ad hoc networks as shown in Figure 3. Routing protocols can be classified into three major categories based on how and when routes are established, these types are:

1- Proactive or Table Driven routing.
2- Reactive or On-Demand routings.
   - Source Routing.
   - Hop-by-hop Routing.
3- Hybrid Routing Protocol.



In proactive or table-driven routing protocols, each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network by sending control messages periodically between the hosts which update their routing tables (Hassnawi *et al*. 2012). Reactive or on-demand routing protocols create routes only when desired by the source node, hence the term on-demand protocols. When a node requires a route to a destination, it initiates a route discovery process within the network. After the route between the source and destination is established the source node starts to send its packets via the established route to the destination. The reactive protocols can be classified into two categories: hop-by-hop routing and source routing. In hop-by-hop routing protocols, forwarding packets forming the source to the destination are based on hop-by-hop decision making, as pre-determined in the hop-by-hop routing table. In hop-by-hop, routing each node is concerned about the next hop towards its destination. In these routing protocols, routes can be adapted frequently, especially in highly dynamic networks with fewer overheads. On the other hand, in source routing protocols, the source draws the data packets' path from the source to the destination and puts this path on the header of the data packet. Routers between the source and the destination forward the packet, according to the path determined by the source. While the hybrid routing protocol algorithms are a mixture of proactive and reactive algorithms. The nodes in the hybrid routing protocols are proactive with all nodes within the same zone and reactive with all nodes outside the zone.

Moreover, another category for routing protocols termed as neighbors based route decision protocol in which routing protocols rely on trusted neighbors to select the best route. Each of which has its pros and cons that can be briefed comparatively in term of routing information acquisition table 1

Table 1: comparison of routing protocols

Routing protocol	Most common protocols	Requirements	Strength	weakness
Proactive (table-driven)	-DSDV (destination sequence distance vector). (Perkins and Bhagwat, 1994) -OLSR (optimized link state routing). (Jacquet *et al*. 2001) -FSR (fisheye state routing) (Chandra and Thakur, 2015)	Frequently updates (neighboring nodes+ accessible nodes+ total hops to destination) to check the possible change in MANET topology.	Attacking detected faster	Higher overhead and bandwidth consumption whenever: -topology change. -additional mobile node joined.
Reactive (on-demand)	-AODV (ad-hoc on-demand distance vector).(Perkins *et al*. 2003) -DSR (dynamic source routing).(Johnson and Maltz, 1996; Bakht, 2016) - TORA (temporally-ordered routing algorithm) (Aburada *et al*. 2006)	Routing information reactively updates once MANET topology modified	-Bandwidth consumption. -Delay in packet transmission.	Attacking node is identified late.
Hybrid	-ZRP (zone routing protocol).(Chandra and Thakur, 2015) - (ZHLS) (zone based hierarchical link state routing protocol)(Chandra and Thakur, 2015) -HWMP (hybrid wireless mesh protocol)(Chandra and Thakur, 2015)	1-performs proactive routing behavior to acquire anonymous routes. 2- Performs reactive routing behavior when a modification in MANET occurs.	-Less bandwidth consumption. Due to low control overhead. -secure and accurate to detect attacks. -the better communication links	unknown

Revision of related efforts:

As known that inherent defects in the construct of routing protocols in MANET make the security prone to black hole aggressive action that motivates attentive researchers in turn to suggest related schemes. Based on the literature we observed that solution approaches can fall under several categories that are briefly demonstrated and examples in each category are given in the coming subsections. The researchers exploit common simulators to validate their proposals were in states pre and later adopting the suggested solution are differentiated based on certain network metrics. But the most comparable used are: 'packet delivery ratio' as a reflection of total data delivered to the destination, 'end-to-end delay' as an indication the average time required to deliver a packet to a destination, 'routing overload' which refers to a number of additional messages utilized. Based on the literature we observed that solution approaches could fall under several categories that are briefly demonstrated and with examples of each category are given in the coming subsections.

1. Malicious behavior category is related to proposing solutions after discriminating black hole attack into single and cooperative based on a number of adversary nodes.

A. Single black hole attack combat schemes:

Samples of the single black hole are discussed below and compared based on main characteristics are listed in table 1.

AODV based black hole attacker deception and isolation (Banerjee et al. 2014):

In 2014, Banerjee brought out an intelligent way in which the source node is fully responsible to deceivably catch and isolate black hole node. Source node floods fake RREQ contains intentionally wrong sequence id of the goal that is much greater than the real goal's sequence id. Based on the nature of aggressive node to answer with maximum sequence it is worthy mentioned that no one of the involved nodes who received the fake RREQ will answer with RREP because no one of them has matching goal sequence id. Thus, the only RREP that contains sequence id greater than that in the fake RREQ belongs to a black hole node. Consequently, the source stores IP add of the black hole node to block any further participation. The source node isolates the aggressive node by announcing its IP add to all participating nodes before performing the traditional functionality of AODV.

DSR cash based black hole attack blockage (Kshirsagar and Patil, 2013):

Kshirsagar and Patil (2013), suggested a fluent DSR based black hole prohibition method, which exploits route cashing function of DSR routing protocol in mobile ad-hoc network. The authors showed that during searching for path process once a black hole-intention is detected the suggested method immediately crashes the ID of the black hole node in an add-to-route activity where all routes are cashed for a limited time in order to analyze them and reject any route leads to that black hole node. Network simulator 2.29 manifested that end-to-end delay after employing the suggested method is negligible and moderate performance is achieved in terms of throughput and jitter. Based on the simulation outcomes it is noted that the performance is stable even with growth in network range and increasing number of joining nodes.

Table 2: Compare of single black hole attack solutions

Schemes	Routing Protocol	Simulator	Publishing Year	Strength	Defects
Subhashis Banerjee method (Banerjee *et al*. 2014)	AODV	Not mentioned	2014	-No modification in packet structure of AODV. -No extra control packets. -Can be employed to discover single and cooperative black hole attack.	-Slightly extra overhead in routing path detection stage.
Online monitoring based black hole attack repulsing (Kshirsagar and Patil, 2013)	AODV	NS2	2013	-PDR increased with high mobility	-Routing overhead increased due to control and notification packets
Receiving reply approach based AODV enhancement(Chou *et al*. 2015)	AODV	NS2	2015	-immediately discovers black hole attacker. -better PDR. - minimal delay -less congested traffic during the processing.	-additional overhead due to the control message to saving replies in the cashing table as well as waiting time variable.
DSR routing cash based black hole attack blockage (Kshirsagar and Patil, 2013; Bakht, 2016)	DSR	NS2	2013	- No extra time consumption for route cashing. - reduced delay. - Obviously minimized dropped packets. Stable performance even with scalability in network size and joined nodes	unknown

Online monitoring based black hole attack repulsing:

Kshirsagar and Patil (2013), proposed a real-time solution to identify as well as to stop black hole adversary. A node adjoining to the suspicious node plays the key role in this solution. The proposed method

involves two phases: real-time observation phase and warning phase. Real-time observation phase begins once a node answers the source node with RREP containing large sequence id. Immediately the source node identifies that node as probable attacking node namely doubtful. The adjoining node spies on a doubtful node next to it based on an order taken from the source node. The adjoining node enters an indistinctive mode to be able to spy on its doubtful neighbor node by tracing all packets transmitted by the probable attacker. The adjoining node manages two counters: (fcount) to count how many packets forwarded from the doubtful node while (rcount) to count how many packets received to the doubtful node. The fcount increases every time adjoining node forwards packets to the doubtful node. If doubtful node forwards that packet, the rcount will increase. The adjoining node keeps transmitting packets to the doubtful node up to reaching threshold average number specified in each network. If rcount equals zero then the doubtful node is definitely a black hole because of packets dropping behavior. Threshold average number indicates to maximum packets sent to a doubtful node to confirm it is a black hole node Warning phase begins immediately after black hole node is recognized by adjoining node, which will send a warning packet to all participating nodes concerning the malicious node. Results from network simulator 2.34 displays that PDR of the proposed solution is 75% under black hole attack condition. Routing overhead is somewhat high due to control packets and notification message.

Receiving reply approach based AODV enhancement (Choudhury et al. 2015):

Debarati Roy Choudhury *et al*. (2015), suggested an approach protects the default behavior of reliable nodes including the goal nodes from any probable tampering in the future through amendments made on data structure of essential AODV routing protocol which involve three extra elements; a table to cash all reply packets received to source node, a specific timer for reply packets to be cashed in the table waiting as well as an entry for malicious node. Moreover, the suggested approach includes adding extra function to work within the source node namely pre-receive reply function that can help the source node to choose the reply that has second maximum goal sequence number because the first belongs to the confirmed black hole node. simulation results from NS2 prove that the suggested approach achieves 60.877% better PDR and less delay due to the early attack identification and less throughput in comparison with the results of conventional AODV under black hole attack.

B. Cooperative black hole attack combat schemes:

The schemes and algorithms that impressively succeeded in combating single black hole danger show setback in fighting cooperative black hole danger that prompts the researcher to look for different solutions (Oliveira *et al*. 2009; Tseng *et al*. 2011). Table 3 comparatively shows patterns of schemes to tackle black hole action performed by a group of attacking nodes.

Prevention Of Co-Operative Black Hole Attack (PCBHA) Based on fidelity threshold Scheme (Tamilselvan and Sankaranarayanan, 2008):

In 2008, Tamilselvanand Sankaranarayanan, suggested a scheme as an improvement of essential AODV routing protocol to reveal the collaborative black hole nodes and insulate them from connecting with other reliable nodes. The proposed PCBHA rely on 'Fidelity table' the core idea is to check nodes authenticity by setting a fidelity level for each node. Fidelity level gives an indication that the node responds to the initial request of the source node is authenticated or black hole attacker. Fidelity table cashes fidelity level and hop count for every partaking node. The fidelity level increases every time a node partakes otherwise fidelity level decreases. It is worth mentioning that the goal node sends acknowledge packet every time receives a request from the source node and its fidelity level rises. After a number of requests from the source node for threshold time the node with zero fidelity level is flagged as black hole attacker and insulate it from other nodes. The node poses highest average of fidelity level is the best to carry out data packets to the goal node. When nodes equalize in an average of fidelity level then the node with less hop count is considered. The outputs of Global Mobile simulator shows that PCBHA achieves 90% packet delivery ratio in comparison with 30% achieved in essential AODV. In contrast, PCBHA raised routing overhead consequently to fidelity control packets transacted to assure more secure data transfer.

Bait DSR (BDSR) On Basis Of Hybrid Routing Scheme (Tsou et al. 2011):

Po-Chun Tsou (2011), give a new defending scheme against cooperative black hole attack termed as Bait DSR (BDSR). The presented mechanism includes table-driven and on-demand routing protocols to build a hybrid routing protocol but essentially relies on DSR reactive routing: the defending solution is simply summarized as below.

Before route detection phase starts, the source node broadcasts bait RREQ packet. The destination address of bait RREQ is unavailable. To prevent probable traffic jam caused by broadcasting bait RREQ packets the proposed BDSR exploit DSR due to limited lifetime of all bait RREQ packets. The aggressive nodes are simply recognized from the start due to the ability of bait RREQ to take the fake RREP from black hole node in the

proposed mechanism the address of every responding node is stored in RREP extra field and sent to source node with the RREP packet. Thus, all RREPs from aggressive nodes would be neglected. Afterward, the authors follow DSR route detection process. In case data delivery ratio is bellow pre-specified threshold level the baiting process will be restarted checking the uncertain nodes.

Simulation outputs show that packet delivery ratio (PDR) is 90% higher in comparison with watching dog (WD) scheme and ordinary DSR routing protocol. Communication overhead is less than that in WD but somewhat higher than DSR routing protocol.

Prohibition Of Internal And External Attacks Based On Secure Way Route (SWR) Scheme (Rajeshwar and Narsimha, 2015):

Rajeshwar and Narsimha (2015), design a fresh Secure Way Route scheme (SWR) to discover internal and external attacking nodes. SWR uses three security mechanisms to discriminate between internal and external attacks that are Certificate Acquisition (CA), Secure Route Discovery as well as Secure Data Routing. The scheme employs Certificate Authority CA to detect the internal attacks and employs symmetric and asymmetric encryption to secure data packets against external attacks. SWR encrypts routing packets using CA to protect routing information from tampering or being fake. In the certificate acquisition stage, the CA grants set of certificates for any reliable node namely, certified authority public key CApub_key , address for the node Nadd, private and public key respectively Npvt_key and Npub_key before partaking the network thus any illegitimate intruder can be easily detected and isolated this secures the reliable nodes from internal attacks. In secure route discovery stage, SWR firstly secures route detection operation by generating session key Skey based on Diffie-Hellman algorithm then gives signature to the encrypted message Sm_sig and also generates cipher to the encrypted message namely Emsg utilizing the CApub_key. Again, CApub_key is employed to re-encrypt the message before broadcasting. The reason of doubled encryption is to raise the level of security from internal and external attackers. SWR scheme compares among the security parameters to determine the safe route during route detection of each node. In secure data routing stage, the source node builds unique secret key SCkey based on DSKey the key received from destination node through route detection session. Then the source performs data encryption utilizing SCkey before sending to the destination. The authors validate the performance of SWR protocol using GloMoSim simulator in comparison with AODV (Rajeshwar and Narsimha, 2015), SAODV (Kumar and Das, 2008), SRAODV (Zapata and Asokan, 2002) as well as ARAN (Sanzgiri *et al*. 2002) . The simulation outputs show that SWR achieves 25% better PDR whereas other protocols show 10-20% when 40% attacking nodes. End-to-end delay is less in SWR and ARAN. SWR achieves lowest routing overhead. SWR through double shielded message makes security breakage difficult.

Table 3: Compare Of Cooperative Black Hole Attack Solutions

Schemes	Routing Protocol	Simulator	Publication Year	Results	Defects
PCBH (Abedi, 2008)	AODV	GloMoSim	2008	-PDR is 90% comparing with 30% AOVD. -less link breakage even with high speed and high packet traffic(Abedi, 2008).	Higher control overhead than AODV.
BDSR (Tsou *et al*. 2011)	DSR	QualNET	2011	PDR of BDSR is normally higher than 90% (Tsou *et al*. 2011)	overhead is somewhat higher than DSR, but lower than WD approach
SWR (Rajeshwar and Narsimha, 2015)	AODV	GloMoSim	2015	-Highly secured through double shielded security. -PDR is 25% higher than AODV	Link failure when high mobility.

2. Performance evaluation category:

It is related to comparing the performance of proposed scheme with other schemes against black hole attack or comparing scheme's performance under different kinds of attacks.

Performance assessment of HWMP against network layer threats in MANET:

The work of Aproova (Chandra and Thakur, 2015) can be considered a good example of two classes of performance evaluation category because they assess the performance of hybrid wireless mesh protocol (HWMP) with respect to recently used routing protocols AODV and ZRP against three aggressive and hard to detect attacks threaten routing layer attacks. Jellyfish attack as a passive attack due to the ability to tamper the packet by reordering it, block it or even delay it without changing packet's value or taking place in the structure of the network. Thus, has no effect on packet transmitting, gray hole attack due to its ability to drag the data packets discard some of it but not all causing denial of service problem as well as routing malfunctioning and black hole attack due to its ability to swallow all data packets without any chance to forward it. Performance

assessment is made using network simulator (NS2) and its outputs prove that routing packets are better in HWMP, which means raised packet transmission in comparison with ZRP. In addition, it results that AODV performance is much lower than HWMP and ZRP in terms of throughput, mean end-to-end and PDR. However, AODV performs well against jellyfish in contrast to other two hybrid routing techniques.

Performance evaluation of ERID-AODV against many black hole adversaries (Salem and Hamamreh 2016):

In 2016, (Salem and Hamamreh, 2016) draw the attention on an efficient mechanism that performs better in terms of PDR and throughput and lessens delay of delivery from end to end unlike preceding proposals of black hole fighting mechanisms. This is achieved through some enhancements on predecessor proposed mechanism namely RID-AODV(Shree and Ogwu, 2013). The idea is based on generating 'dynamic blacklist' in every node and prevent transactions with the nodes in the blacklist. The blacklisting decision is made based on a threshold value, which represents occurrence times of mismatched hashing value from the suspicious nodes. Afterward, the authors assessed the efficiency of Enhanced RID-AODV comparatively with RID-AODV which essentially exploits the advantage both RAODV (Kim *et al*. 2006) along with IDSAODV (Dokurer *et al*. 2007) and basic AODV. The results of network simulator demonstrate that ERID-AODV recognizes and mitigates black hole attacking nodes with obviously highest PDR, throughput due to utilizing dynamic blacklist and threshold value that lessen losing packets affected by black hole attacking nodes. In addition, ERID-AODV achieves a very less average delay in delivery due to dynamic blacklist helps to transact data packets to pure nodes and prevent routing the packets to the black holes in the dynamic list.

Comparative study on MANET performance using AODV,OLSR, and ZRP against black hole attack (Kaur et al. 2013):

Harjeet Kaur (2013), investigate the effect of a black hole on MANET for different network conditions using AODV, OLSR, and ZRP routing protocols. The comparison is made for every protocol free and under attack conditions. The comparison is made based on PDR, jitter, throughput and delay. Simulation results of QualNet5.1 show that AODV under black hole attack is minimally impacted among other protocols with increasing number of adversary black hole nodes. AODV achieves better PDR and throughput less jitter end-to-end delay.

Table 4: performance evaluation

Scheme	Compare	Simulator	Publication year	Results	Defects
HWMP (Chandra and Thakur, 2015)	ZRP, AODV	NS2	2015	-better PDR. -raised throughput - efficient routing packets (Chandra and Thakur, 2015)	Fail to tackle Jellyfish attack in contrast to black hole and gray hole attacks
ERID-AODV	AODV, RID-AODV(Shree and Ogwu, 2013), RAODV(Kim *et al*. 2006), IDSAODV(Dokurer *et al*. 2007)	NS2	2016	Dynamic blacklist threshold based elevates PDR to almost 80% and throughputs to 40% even with increasing attacking nodes and reduces end-to-end delay (Shree and Ogwu, 2013)	RID-AODV shows better performance in term of average end-to-end delay with increasing attacking nodes.
Comparative Study of Harjee (Kaur *et al.* 2013)	AODV, OLSR, ZRP	QualNet5.1	2013	AODV is less affected by increasing no. of black hole attackers. AODV performs better than ZRP, and OLSR under and free of attack.(Kaur *et al.* 2013)	

Detection category is related to fighting black hole attack, which can be classified into Amendments to the conventional secure routing protocol or introducing the fresh scheme. Samples of detection category are summarized in table 5.

AODV improvement approach of Kumar's (Kumar and Kumar, 2015):

Vimal Kumar in 2015, made an amendment to elementary AODV and come up with an approach to reveal black hole threat with a decreased communication cost in MANET by assigning table namely CCRT to manage reaching answers to source from unconfirmed nodes. Beyond using Network Simulator 2.43, the introduced approach has proven to be more accurate than previous solutions to reveal black hole attack in MANET as PDR

shows 96% higher than elementary AODV under attack of black hole node. Moreover, the throughput is enhanced by 336.14 kbps than that of AODV 314.32 kbps.

Control packets based scheme (Dhaka et al. 2015):

Arvind Dhaka in 2015, introduced a fresh scheme adapts AODV routing protocol to simply discriminate and rapidly isolate aggressive node. the source node gives Cseq to every surrounding node and compares it with Rreq reflected from the node if Rseq=Cseq then the node is safe otherwise it is malicious based on the fact that any malicious node replies the source with maximum sequence value (Jhaveri *et al*., 2012). The rapid attack detection nature refers to two reasons control packets are sent early in AODV-MAC layer and the scheme only compares the premier entry where the maximum sequence id of the malicious node is located in Cseq-table regardless the rest entries. The scheme achieves lower end-to-end in comparison with previously proposed schemes and 57% PDR as demonstrates in NS2 simulation charts.

Various RREP-based route decision (Lo and Liu, 2013):

Nai-Wei Lo *et al* (2013) innovate a cooperative black hole recognition mechanism namely CBAODV. The basic idea of CBAODV is that the source node at the minimum need to check on two RREP from diverse nodes concerning same goal node to make a decision to the preferable secured path to route the data packets to the goal node even if the chosen route is not the fastest to the goal. The source node confirms the route decision based on control packet generated by CBAODV. The QualNet5 simulation outputs show that PDR using CBAODV is increased 70-80% while PDR 20-40% using basic AODV under violation of cooperative black hole nodes. The end-to-end level is upper when employing CBAODV due to the time waiting for all RREP packets to reach from various nodes about second routing path in advance to choose the preferable path.

Shortest secure algorithm (Ghathwan and Yaakub, 2014):

In 2014, Ghathwan and Yaakub recommended a technique to block black hole cooperative nodes after some adjustments on original AODV namely SSP-AODV which aims to explore the safest shortest distance route to the goal node with less overhead. SSP-AODV exploits the algorithm of Floyd-Warshal (Chen, 1990) to estimate the length between the adjoining nodes during RREQ and RREP time interval. Based on the fact that the algorithm of Floyd-Warshal is unable to find the shortest path to the goal node. SSP-AODV takes the advantage of heuristic search technique A* to predict the shortest route between source and goal nodes. The reason behind combining those two techniques is to minimize overhead and secure the routing process. In proposed SSP-AODV whenever source node gets RREP from one or more surrounding nodes, it postpones sending a packet immediately till routing time ends. Then after, source node holds on for a short interval. If the hold on time equals or exceeds threshold time then the value of hop count is calculated. The desired path is confirmed secure if the value of hop count is identical in RREQ and RREP tables all altogether, otherwise. The path will be canceled from the routing table. SSP-AODV mechanism selects 'shortest secure path' from 'SP-value' in both tables RREQ and RREP. After using NS2.23 simulation results under the condition of cooperative black hole attack stated that SSP-AODV decreases packets close to 22.98% instead of 28.32% when AODV is employed. The end-to-end average delay is minimized to 11.42% as compared with 29% in AODV. PDR

Table 5: black hole detection category

Approach	Routing Protocol	Simulator	Publication Year	Results	Defects
AODV improvement approach of Kumar's (Kumar and Kumar, 2015)	AODV	NS2	2015	-less communication cost. -accurate black hole detection. -raised PDR, throughput.(Kumar and Kumar, 2015)	unknown
Control packets based scheme (Bhalodiya and Vaghela, 2015	AODV	NS2	2015	-Rapidly reveals a black hole and gray hole attacks. -Less end-to-end delay. (Bhalodiya and Vaghela, 2015).	Performance reduction at high node mobility rates and cooperative black hole attack.
Various RREP-based route decision (Lo and Liu, 2013)	AODV	QualNet5	2013	-PDR increased up to 2.6 times than AODV	Performance is somewhat slow down due to path decision time.
SSP-AODV(Ghathwan and Yaakub, 2014)	AODV	NS2	2014	-fewer packets lose. -less end to end delay	A slight reduction in PDR due to using security algorithm.

Conclusion:

In mobile ad hoc networks (MANET), nodes rely on each other to keep the network connected. Thus, unlike traditional wireless solutions, such networks do not require any pre-existent (fixed) infrastructure, which minimizes their cost and deployment time. Therefore, security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of the network. The availability of network services, confidentiality, and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battlefield situation for the MANETs against the security threats. Black hole attack is the very important to type that became as an interesting point of many researchers.

Routing protocols enable multi-hop communications in ad hoc networks. To achieve availability, routing protocols should be robust against both topology changes and malicious attacks. It can be concluded from the researchers' work that there are two sources of black hole threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat come from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures. Therefore, this work addressed the main categories of black hole malicious behaviors as well as the fighting techniques used to decrease the effects of this type of attack categories. In this work, we compare the effect of each defense's technique on the network performance different evaluation metrics and under different network environments. It can be concluded from the literature that increasing network defense against black hole attacker come at the expense of increasing network overhead and the transmission time delay which leads to decrease the PDR, consequently degraded network performance.

The effectiveness of each defense's mechanism depends on the type of routing algorithm used. In this context, at using proactive or table driven algorithms, the defense mechanism will be strong to detect the attacker faster than using reactive or on demand routing algorithms but this strength comes at the expense of exploiting the bandwidth, consequently affecting network performance. Therefore, using hybrid routing algorithm decreases the effects of bandwidth consumption as well as increases network defense against black hole attack.

As future work, research work intends to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage, mobility, increasing a number of the malicious node, increasing the number of nodes and scope of the black hole nodes. Also focusing on resolving the problem of multiple attacks against reactive and proactive routing protocol such as AODV and DSR.

REFERENCES

Abedi, O., Fathy, M. and Taghiloo, J., 2008, March. Enhancing AODV routing protocol using mobility parameters in VANET. IEEE/ACS International Conference on Computer Systems and Applications. pp.:229-235.

Aburada, K., Morita, K., Okazaki, N., Tomita, S. and Park, M.R., 2006, August. Proposal of a robust zone-based hierarchical routing method for ad hoc networks. Asia-Pacific Conference on Communications IEEE., pp:1-5.

Amutha, S. and Kannan Balasubramanian, 2015. Detection and Prevention of Black Hole Attack on MANET Routing Protocols. Australian Journal of Basic and Applied Sciences, 9: 281-289

Bakht, H., 2016. A Comparative Study Of Maoddp With Zrp and Dsr Routing Protocols For Mobile Ad-Hoc Network. Computer Science and Telecommunications, (1), p.47.

Banerjee, S., Sardar, M. and Majumder, K., 2014. Aodv based black-hole attack mitigation in MANET. In Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) Springer International Publishing, pp: 345-352.

Bhalodiya, S. and K. Vaghela, 2015. Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol. International Journal of Computer Applications, 125(4).

Chandra, A. and S. Thakur, 2015. Performance evaluation of hybrid routing protocols against network layer attacks in MANET. Next Generation Computing Technologies (NGCT), 2015 1st International Conference on, IEEE, pp. 239-244

Chatterjee, R. and M. Routray, 2011. Black Hole Combat Using Node Stability System in MANET. Signal Processing and Information Technology, Springer, pp: 249-254.

Chen, W.-K., 1990. "Theory of nets: flows in networks."

Choudhury, D.R., Ragha, L. and Marathe, N., 2015. Implementing and Improving the Performance of AODV by Receive Reply Method and Securing it from Black Hole Attack. Procedia Computer Science, 45: 564-570.

Dhaka, A., Nandal, A. and Dhaka, 2015. "Gray and Black Hole Attack Identification Using Control Packets in MANETs." Procedia Computer Science 54: 83-91.

Dokurer, S., *et al*., 2007. "Performance analysis of ad hoc networks under Blackhole attacks. Southeast Con, " Proceedings IEEE 148: 153.

Ghathwan, K.I. and A.R.B. Yaakub, 2014. An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET. Recent Advances in Soft Computing and Data Mining, Springer, pp: 121-131.

Hassnawi, L., *et al*., 2012. Performance analysis of various routing protocols for motorway surveillance system cameras' network. International Journal of Computer Science, 9: 52-62.

Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L. Optimized link state routing protocol for ad hoc networks. InMulti Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International 2001, pp: 62-68.

Jamali, S.B.S., 2015. A survey over black hole attack detection in mobile ad hoc network. International Journal of Computer Science and Network Security (IJCSNS) 15(3): 44.

Jhaveri, R.H., S.J. Patel and D.C. Jinwala, 2012. January. A novel approach for the gray hole and black hole attacks in mobile ad hoc networks. Second International Conference on Advanced Computing & Communication Technologies, IEEE., p: 556-560.

Johnson, D.B. and D.A. Maltz, 1996. Dynamic source routing in ad hoc wireless networks. Mobile computing, Springer, pp: 153-181.

Kamatchi, V. and R. Mukesh, 2013. Securing Data from Black Hole Attack Using AODV Routing for Mobile Ad Hoc Networks. Advances in Computing and Information Technology, Springer, pp: 365-373.

Kaur, H., Bala, M., and Sahni, V., 2013. Study of Blackhole Attack Using Different Routing Protocols in MANET. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2(7): 3031-3039.

Kim, C., Talipov, E. and Ahn, B., 2006, August. A reverse AODV routing protocol in ad hoc mobile networks. In International Conference on Embedded and Ubiquitous Computing Springer Berlin Heidelberg, pp: 522-531.

Kshirsagar, D. and A. Patil, 2013. Blackhole attack detection and prevention by real-time monitoring. Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on, IEEE, pp: 1-5.

Kumar, V. and M.L. Das, 2008. Securing Wireless Sensor Networks with Public Key Techniques. Ad-hoc & Sensor Wireless Networks, pp: 5.

Kumar, V. and R. Kumar, 2015. An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network. Procedia Computer Science, 48: 472-479.

Lo, N.-W. and F.-L. Liu, 2013. A secure routing protocol to prevent cooperative black hole attack in MANET. Intelligent Technologies and Engineering Systems, Springer, pp: 59-65.

Marti, S., Giuli, T.J., Lai, K., and Baker, M., 2000, August. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking ACM, pp: 255-265.

Mbarushimana, C. and A. Shahrabi, 2007. Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. Advanced Information Networking and Applications Workshops, AINAW'07. 21st International Conference on, IEEE, Vol. (2): 679-684

Mistry, N.H., Jinwala, D.C. and Zaveri, M.A., 2009. MOSAODV: solution to secure AODV against black hole attack. IJCNS)International Journal of Computer and Network Security, 1(3): 42-45.

Nadeem, A. and M. Howarth, 2013. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. Telecommunication Systems, 52(4): 2047-2058.

Nandakumar, R. and Nirmala, K., 2016. Security Challenges in Mobile Ad Hoc Network- A Servey. Australian Journal of Basic and Applied Sciences, 10: 654-66

Navamani, T. and P. Yogesh, 2015. Secure Efficient Routing against Packet Dropping Attacks in Wireless Mesh Networks. Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, Springer, pp: 673-686.

Oliveira, R., Bhargava, B., Azarmi, M., Ferreira, E.W.T., Wang, W. and Lindermann, M., 2009, September. Developing Attack Defense Ideas for Ad Hoc Wireless Networks. In 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009)(in Conjunction with IEEE SRDS 2009), New York, USA, Vol (27).

Pani, N.K. and S. Mishra, 2014. Secure Hybrid Routing for MANET Resilient to Internal and External Attacks. ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I, Springer, Vol (I): 449-458.

Patel, B. and K. Trivedi, 2014. Improving AODV Routing Protocol against Black Hole Attack based on MANET. IJCSIT) International Journal of Computer Science and Information Technologies 5(3): 3586-3589.

Perkins, C., Belding-Royer, E. and Das, S., 2003. Ad-hoc on-demand distance vector (AODV) routing, No. RFC 3561.

Perkins, C.E. and P. Bhagwat, 1994. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM computer communication review, ACM. 24(4): 234-244.

Rajeshwar, J. and G. Narsimha, 2015. "Secure way routing protocol for mobile ad hoc network." Wireless Networks, pp: 1-10.

Salem, A.-R. And D.R. Hamamreh, 2016. Efficient Mechanism For Mitigating Multiple Black Hole Attacks In Manets. Journal of Theoretical and Applied Information Technology, 83(1).

Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C. and Belding-Royer, E.M., 2002, November. A secure routing protocol for ad hoc networks. In Network Protocols. Proceedings. 10th IEEE International Conference on IEEE, pp: 78-87.

Shree, O. and F.J. Ogwu, 2013. A proposal for mitigating multiple black-hole attacks in wireless mesh networks, 5(4).

Suryawanshi, R. and Tamhankar, S., 2012. Performance analysis and minimization of black hole attack in MANET. International Journal of Engineering Research and Applications (IJERA), ISSN, pp: 2248-9622.

Tamilselvan, L. and V. Sankaranarayanan, 2008. Prevention of cooperative black hole attack in MANET. Journal of networks, 3(5): 13-20.

Thanvi, T., Arora, N., and Vyas, P. 2015. Literature Survey of MANET under Blackhole and Gray hole attack. International Journal of Advanced Research in Computer and Communication Engineering, 4(9).

Tripathi, V.K. and S. Venkaeswari, 2015. Secure communication with privacy preservation in VANET-using multilingual translation. Communication Technologies (GCCT), 2015 Global Conference on, IEEE, pp: 125-127.

Tseng, F.-H., Chou, L.D. and Chao, H.C., 2011. A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1): 1.

Tsou, P.C., Chang, J.M., Lin, Y.H., Chao, H.C. and Chen, J.L., 2011, February. Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs. In Advanced Communication Technology (ICACT), 2011 13th International Conference on IEEE, pp: 755-760.

Umang, S., Reddy, B.V.R. and Hoda, M.N., 2010. Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption. IET communications, 4(17): 2084-2094.

Verma, A.K., Joshi, R.C. and Dave, M.G., 2008. Design and development of a routing protocol for mobile ad hoc (Doctoral dissertation).

Wu, B., Chen, J., Wu, J. and Cardei, M., 2007. A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security . Springer US, pp: 103-135.

Yang, B., Yamamoto, R. and Tanaka, Y., 2012, February. Historical evidence-based trust management strategy against black hole attacks in MANET. In Advanced Communication Technology (ICACT), 2012 14th International Conference on IEEE, pp: 394-399.

Zapata, M.G. and N. Asokan, 2002. Securing ad hoc routing protocols. Proceedings of the 1st ACM workshop on Wireless security, ACM, p:1-10