Human-centric Computing and Information Sciences
a SpringerOpen Journal

RESEARCH Open Access

A survey of black hole attacks in wireless mobile ad hoc networks

Fan-Hsun Tseng[1], Li-Der Chou[1] and Han-Chieh Chao[2,3,4*]

* Correspondence: hcc@niu.edu.tw
[2]Department of Electronic Engineering, National Ilan University, Taiwan
Full list of author information is available at the end of the article

Abstract

The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes. In this paper, we survey the existing solutions and discuss the state-of-the-art routing methods. We not only classify these proposals into single black hole attack and collaborative black hole attack but also analyze the categories of these solutions and provide a comparison table. We expect to furnish more researchers with a detailed work in anticipation.

Keywords: mobile ad hoc networks, routing protocols, single black hole attack, collaborative black hole attack

1. Introduction

Wireless mobile ad hoc network (or simply *MANET* throughout this paper) is a self-configuring network which is composed of several movable user equipment. These mobile nodes communicate with each other without any infrastructure, furthermore, all of the transmission links are established through wireless medium. According to the communication mode mentioned before. MANET is widely used in military purpose, disaster area, personal area network and so on [1]. However, there are still many open issues about MANETs, such as security problem, finite transmission bandwidth [2], abusive broadcasting messages [3], reliable data delivery [4], dynamic link establishment [5] and restricted hardware caused processing capabilities [6].

The security threats have been extensively discussed and investigated in the wired and wireless networks [7], the correspondingly perplexing situation has also happened in MANET due to the inherent design defects [8]. There are many security issues which have been studied in recent years. For instance, snooping attacks, wormhole attacks, black hole attacks [9], routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, distributed DoS (DDoS) attacks, et cetera [10]. Especially, the misbehavior routing problem [11] is one of the popularized security threats such as black hole attacks. Some researchers propose their secure routing idea [12-15] to solve this issue, but the security problem is still unable to prevent completely.

In this paper, we focus on different types of black hole attacks in MANET which can be divided into ordinary black hole attack and collaborative black hole attack.

Moreover, several detection schemes are discussed clearly and comparably. The evaluation metrics of routing protocol include packet delivery ratio (PDR), mobility variation with total number of errors, packet routing overhead, end-to-end delay by varying in node density [16].

In the following, we first introduce different kinds of routing protocols in Sec. 2, which includes proactive routing, reactive routing and hybrid routing protocols. In Sec. 3 and Sec. 4, we respectively classify the black hole attacks from their malicious operating actions into black hole attacks and collaborative black hole attacks, and also anatomize the misbehavior to provide the comparisons between related literatures in both sections. Finally, we conclude this survey in Sec. 5.

2. Background

There are plenty and different routing protocols in MANET and kinds of investigations have been completed in recent decades [17,18]. In this section, we introduce the famous and popular routing protocols in MANET. Before a mobile node wants to communicate with a target node, it should broadcast its present status to the neighbors due to the current routing information is unfamiliar. According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing.

2.1. Proactive (table-driven) Routing Protocol

The proactive routing is also called table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbors. Each node needs to maintain their routing table which not only records the adjacent nodes and reachable nodes but also the number of hops. In other words, all of the nodes have to evaluate their neighborhoods as long as the network topology has changed. Therefore, the disadvantage is that the overhead rises as the network size increases, a significant communication overhead within a larger network topology. However, the advantage is that network status can be immediately reflected if the malicious attacker joins. The most familiar types of the proactive type are destination sequenced distance vector (DSDV) [19] routing protocol and optimized link state routing (OLSR) [20] protocol.

2.2. Reactive (on-demand) Routing Protocol

The reactive routing is equipped with another appellation named on-demand routing protocol. Unlike the proactive routing, the reactive routing is simply started when nodes desire to transmit data packets. The strength is that the wasted bandwidth induced from the cyclically broadcast can be reduced. Nevertheless, this might also be the fatal wound when there are any malicious nodes in the network environment. The weakness is that passive routing method leads to some packet loss. Here we briefly describe two prevalent on-demand routing protocols which are ad hoc on-demand distance vector (AODV) [21] and dynamic source routing (DSR) [22] protocol.

AODV is constructed based on DSDV routing. In AODV, each node only records the next hop information in its routing table but maintains it for sustaining a routing path from source to destination node. If the destination node can't be reached from the source node, the route discovery process will be executed immediately. In the

route discovery phase, the source node broadcasts the route request (RREQ) packet first. Then all intermediate nodes receive the RREQ packets, but parts of them send the route reply (RREP) packet to the source node if the destination node information is occurred in their routing table. On the other hand, the route maintenance process is started when the network topology has changed or the connection has failed. The source node is informed by a route error (RRER) packet first. Then it utilizes the present routing information to decide a new routing path or restart the route discovery process for updating the information in routing table.

The design idea of DSR is based on source routing. The source routing means that each data packet contains the routing path from source to destination in their headers. Unlike the AODV which only records the next hop information in the routing table, the mobile nodes in DSR maintain their route cache from source to destination node. In terms of the above discussion, the routing path can be determined by source node because the routing information is recorded in the route cache at each node. However, the performance of DSR decreases with the mobility of network increases, a lower packet delivery ratio within the higher network mobility.

2.3. Hybrid Routing Protocol

The hybrid routing protocol combines the advantages of proactive routing and reactive routing to overcome the defects of them. Most of hybrid routing protocols are designed as a hierarchical or layered network framework. In the beginning, proactive routing is employed to completely gather the unfamiliar routing information, then using the reactive routing to maintain the routing information when network topology changes. The familiar hybrid routing protocols are zone routing protocol (ZRP) [23] and temporally-ordered routing algorithm (TORA) [24].

3. Single Black Hole Attack

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the mobile ad hoc networks [25]. An example is shown as Figure 1, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem. The most critical influence is that the PDR diminished severely.

In the following, different detection schemes for single black hole attack are presented in a chronological order. The comparisons of different schemes are shown in Table 1.

3.1. Neighborhood-based and Routing Recovery Scheme [26]

Bo Sun *et al.* use AODV as their routing example, and claim that the on-demand routing protocols such as DSR are also suitably applied after a slightly modified. The

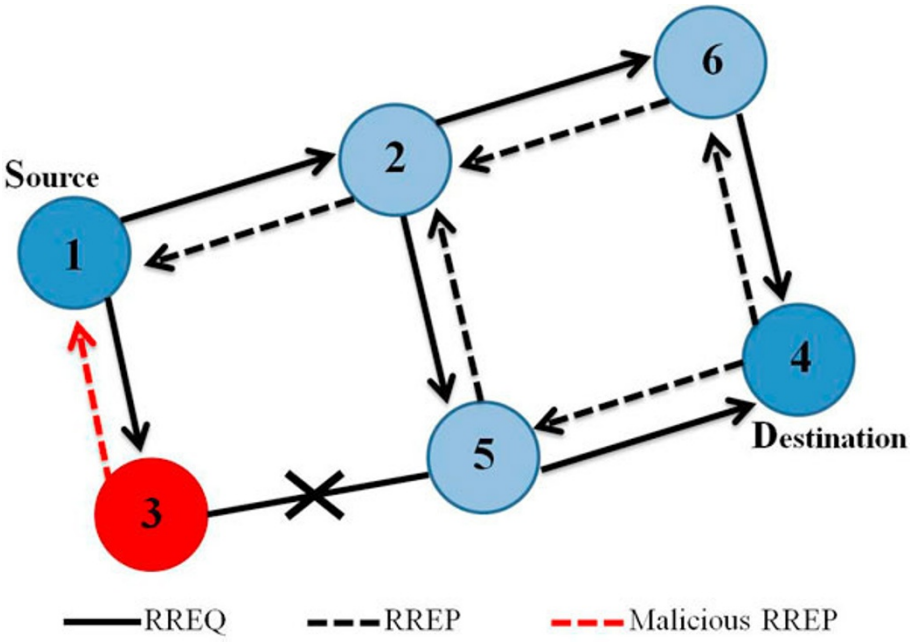

Figure 1 The single black hole problem. Figure 1 is an example of single black hole attack in the mobile ad hoc networks [25]. Node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.

detection scheme uses on a neighborhood-based method to recognize the black hole attack, and a routing recovery protocol to build the correct path. The neighborhood-based method is employed to identify the unconfirmed nodes, and the source node sends a *Modify_Route_Entry* control packet to destination node to renew routing path in the recovery protocol.

In this scheme, not only a lower detection time and higher throughput are acquired, but the accurate detection probability is also achieved. To deserve to be mentioned, the routing control overhead does not increase in Bo Sun *et al.*'s proposal. However, this scheme is useless when the attackers cooperate to forge the fake reply packets.

3.2. Redundant Route Method and Unique Sequence Number Scheme [27]

Mohammad Al-Shurman *et al.* propose two solutions to avoid the black hole attacks in MANET. The first solution is to find more than one route from the source node to the destination node. In other words, there exist some redundant routes within the routing path, and authors assume there are three routes at least in the scenario. The working flow of redundant route mechanism is described briefly as below. First, the source node sends a ping packet, a RREQ packet, to the destination. The receiver who has a route to the destination will reply this request, and a acknowledge examination is executed at source node. Then the sender will buffer the RREP packet until there are more than two received RREP packets, and transmit the buffered packets after identifying a safe route. It represents that there are at lowest two routing paths coexisting at

Table 1 Comparison of Single Black Hole Attack Detection Schemes

Schemes	Routing protocol	Simulator	Detection type	Publication year	Results	Defects
Neighborhood-based and Routing Recovery [26]	AODV	NS-2	Single detection	2003	The probability of one attacker can be detected is 93%	Failed when attackers cooperate to forge the fake reply packets
Redundant Route and Unique Sequence Number Scheme [27]	AODV	NS-2	Single detection	2004	Verify 75% to 98% of the routes	Attackers can listen to the channel and update the tables for last sequence number
Time-based Threshold Detection Scheme [28]	Secure AODV (SAODV)	GloMoSim	Single detection	2007	The PDR of SAODV is around 90 to 100% when AODV is around 80%	The end-to-end delay increases when the malicious node is away from source node
Random Two-hop ACK and Bayesian Detection Scheme [29]	DSR	GloMoSim-based	Cooperative detection	2007	The true positive rate can achieve 100% when existing 2 witness	The proposed scheme is not efficient when k equals to 3, reducing the true positives
REAct [30]	DSR	-	Single detection	2009	Reduces the communication overhead but enlarges the identification delay	The binary search method is easily expose audit node's information
DPRAODV [31]	AODV	NS-2	Single detection	2009	The PDR is improved by 80-85% than AODV when under black hole attack	A little bit higher routing overhead and end-to-end delay than AODV
Next Hop Information Scheme [32]	AODV	NS-2	Single detection	2010	The PDR is improved by 40-50% and the number of packets dropped is decreased by 75-80% than AODV	Few additional delay
Nital Mistry *et al.*'s Method [33]	AODV	NS-2	Single detection	2010	The PDR is improved by 81.811% when network size varying, and rise 70.877% when mobility varying	Rise in end-to-end delay is 13.28% when network size varying, and rise 6.28% when mobility varying
IDS based on ABM [34]	MAODV	NS-2	Single detection	2010	The packet loss rate can be decreased to 11.28% and 14.76%	Cooperative isolation the malicious node, but failed at collaborative black hole attacks

-: means unmentioned

the same time. After that, the source node recognizes the safe route from the number of hops or nodes, and prevents the black hole attacks.

In the second solution, an idea of unique sequence number is mentioned. The sequence value is accumulated; hence it's ever higher than the current sequence number. In this solution, two values are needed to be recorded in two additional

tables. One is the *last-packet-sequence-numbers* for the last packet sent to every node and the other is for the last packet received. When any packet are transmitted or received, these two tables will be updated automatically. According to these two table values, the sender node can identify whether there is malicious nodes or not.

In the simulation results, these two solutions have less RREQ and RREP numbers than AODV. Furthermore, solution two is better than solution one due to the sequence number included in every packet in the original routing protocol. The communication overhead can be eliminated by this solution because of the inbound cryptography method. Nevertheless, the cooperative black hole attacks can't be detected in both proposed solutions. The redundant route and unique sequence number can be easily broke by two collaborative black hole nodes.

3.3. Time-based Threshold Detection Scheme [28]

Latha Tamilselvan *et al.* propose a solution based on an enhancement of the original AODV routing protocol. The major design concept is setting timer in the *RimerExpiredTable* for collecting the other request from other nodes after receiving the first request. It will store the packet's sequence number and the received time in a *Collect Route Reply Table* (CRRT), counting the timeout value based on the arriving time of the first route request, judging the route belong to valid or not based on the above threshold value. The simulation using global mobile simulator (GloMoSim) shows that a higher packet delivery ratio is obtained with only minimal delay and overhead. But the end-to-end delay might be raised visibly when the suspicious node is away from the source node.

3.4. Random Two-hop ACK and Bayesian Detection Scheme [29]

Djamel Djenouri *et al.* propose a solution to monitor, detect, and isolate the black hole attack in MANETs. In the monitor phase, an efficient technique of random two-hop ACK is employed. The simulation result shows that random two-hop ACK hugely reduces the cost with a higher true and lower false detection than ordinary two-hop ACK scheme. A local judgment approach based on Bayesian technique is penetrated in the detection phase. The proposed Bayesian detection method does not use any periodic packets exchanging, therefore the familiar overhead problem can be eliminated from this solution. And after a mobile node is determined that it is a misbehavior node by the proposed detection scheme, this judgment must be proved by all nodes. Hence, authors propose a witness-based protocol that forces the recognized node to ensure this decision from other nodes. Before isolating the misbehavior node at the same time, the witness-based protocol enforces the detector to gather k witnesses at least. However, the decision of k value is a trade-off problem. A higher k value eliminates the false detection and attack probability, but reduces the detection efficiency, and vice versa.

The simulation shows that the proposed solution can achieve a lower false detection rate and higher true detection rate than watchdog (WD) approach. The solution utilizes cooperatively witness-based verification, nevertheless, it's difficult to prevent collaborate black hole attack for the judgment phase is only running on local side. It might be failed if some malicious nodes deceive the detection node cooperatively.

3.5. Resource-Efficient ACcounTability (REAct) Scheme based on Random Audits [30]

William Kozma Jr. *et al.* propose a reactive misbehavior detection scheme called REAct scheme. When the performance is descended between source and destination node, the REAct is triggered automatically. REAct constitutes of three phases: (a) the audit phase, (b) the search phase and (c) the identification phase. To simply describe the REAct scheme, the target node sends a feedback to the sender when a biggish packet drop ratio is recognized. Then the source node chooses an audit node, and utilizes the bloom filter to produce a behavioral proof. Finally, the segment location of malicious node can be distinguished from comparing the source node's behavioral proof.

The simulation shows that REAct scheme not only reduces the communication overhead, but enlarges the identification delay because REAct is based on reactive DSR routing protocol. Furthermore, there are some critical weaknesses in REAct. First, the REAct is designed for non-cooperative black hole attack only. It's unsuccessful in the collaborative black hole scenario because other malicious node is able to manipulate a fake proof and send to the audit node. Second, the behavioral proof only records the information of transmission packets rather than the nodes. It fails to verify who the producer of the behavioral proof is. Finally, using the binary search method to find the attacker is easily expose audit node's information. The attacker is able to cheat source node by changing its behavior dynamically.

3.6. Detection, Prevention and Reactive AODV (DPRAODV) Scheme [31]

A new control packet called *ALARM* is used in DPRAODV, while other main concepts are the dynamic threshold value. Unlike normal AODV, the *RREP_seq_no* is extra checked whether higher than the threshold value or not. If the value of *RREP_seq_no* is higher than the threshold value, the sender is regarded as an attacker and updated it to the black list. The *ALARM* is sent to its neighbors which includes the black list, thus the RREP from the malicious node is blocked but is not processed. On the other hand, the dynamic threshold value is changed by calculating the average of *dest_seq_no* between the sequence number and RREP packet in each time slot. According to this scheme, the black hole attacks not only be detected but also prevented by updating threshold which responses the realistic network environment.

In the simulation results, the packet delivery ratio is improved by 80-85% than AODV when under black hole attack, and 60% when traffic load increases. The advantage of DPRAODV is that it achieves an obviously higher packet delivery ratio than the original AODV, except for it takes a little bit higher routing overhead and end-to-end delay. But DPRAODV simply detects multiple black holes rather than cooperative black hole attack.

3.7. Next Hop Information Scheme [32]

N. Jaisankar *et al.* propose a security approach which is composed of two parts, detection and reaction. In the first part, the *field_next_hop* is added to the RREP packet. Before source node sends the data packets, the leading RREP packet is examined between intermediate node and destination node. Each node maintains a black identification table (BIT), and the fields in this table are <source, target, current_node_ID, Packet_received_count (PRC), Packet_forwarded_count (PFC), Packet modified count (PMC)>. Then the PMC is updated by tracing the BIT from their neighborhoods. If

the node acts correctly, the corresponding count value multiplies. After that, a malicious node can be found out if the number of receiving packets differentiates from sending packets. The second part is isolating the black hole, thus each node maintains an isolation table (IT) and stores the black node ID. The ID is broadcasted to all nodes in order to eliminate the malicious node by checking the isolation table.

In the simulation result, the packet delivery ratio is improved by 40-50% than AODV when facing attacks, and the number of packets dropped is decreased by 75-80%. Unlike the conventional next hop method, this solution modifies the original RREP packets to collect the information of malicious nodes rather than sending further packets. The proposed solution provides a higher packet delivery ratio and lower packet loss rate than conventional with little additional delay.

3.8. Nital Mistry *et al.*'s Method [33]

Nital Mistry *et al.* add a new table *Cmg_RREP_Tab*, a new timer *MOS_WAIT_TIME* and a variable *Mali_node* to the original AODV routing protocol. The proposed solution is basically modifies an additional function *Pre_ReceiveReply* viz *Packet P*.

The definitions of innovative functions are clarified first. The *RREP_WAIT_TIME* is a time period during the source node sends first RREP packet until receive the RREP control messages. And the *MOS_WAIT_TIME* is half the value of *RREP_WAIT_TIME*. The RREP packets are stored in the newly built table viz. *Cmg_RREP_Tab*. Lastly the *Mail_node* is utilized to record the malicious nodes in order to discard the control message from these nodes.

After introducing the proposed functions, the approach will be briefly described as below. In the first step, the additional function viz. *Pre_ReceiveReply* is executed. The source node analyzes all the RREP packets stored in the *Cmg_RREP_Tab* table. Then the RREP packet is abandoned which has a higher destination sequence number than the source sequence number, and the sender is suspected to be a malicious node. As long as the attacker is identified, the control message coming from it can be ignored. Thus, the RREP packet with the highest destination sequence number is chosen in *Cmg_RREP_Tab* table. The *Mali_node* is maintained continually, and at final the *ReceiveReply* in default AODV is called.

The PDR is improved by 81.811% when the network size varying, while it will rise 70.877% when the node's mobility varying. Comparing with original AODV routing protocol, this solution achieves a higher packet delivery ratio in the simulation results. However, the end-to-end delay is increased unavoidably. The end-to-end delay is rising 13.28% when network size adjusting, and rising 6.28% when mobility adjusting. Furthermore, this approach is also failed to discuss the collaborative black hole attack problem.

3.9. Intrusion Detection System based on Anti-black hole mechanism [34]

Since there is no centralized infrastructure device in MANET and no difficulty to overcome the inborn characteristics, it's challenged to develop an intrusion detection system (IDS). Ming-Yang Su proposes an IDS scheme to solve the selective black hole attacks in MANET, and plants an anti-black hole mechanism (ABM) in all IDS nodes.

The ABM employs two additional tables called RQ table and SN table as shown in Table 2 and Table 3. The RQ table records the RREQ message within IDS node's

Table 2 RQ table

Route			Maximal hop count	Broadcasting nodes	Expiration time
Source	Destination	Src_seq			
1	5	3001	2	2, 4, 5	02:41:12
3	2	5012	4	1, 6	02:44:34

transmission range. The contents including the source and destination ID, source sequence number, maximum hop count value, broadcasting node ID and expiration time. The IDS nodes use SN table to estimate the suspicious values nodes within its transmission range. The components of SN table including the node ID, suspicious values and status. If an intermediate node never broadcasts a RREQ for a route but sends a RREP packet, the suspicious value will be added one in the neighbor IDS node's SN table. Apart from this, another new Block table is added into the original routing table in order to record the list of black holes. The Block table is shown as Table 4.

The basic framework of proposed IDS is introduced as follow. In the beginning, the IDS nodes execute the ABM function in a sniff mode. According to the irregular difference between the routing information transmitted from a dubious node, a value of the suspicious node can be estimated by ABM. If the value exceeds the predefined threshold value, it can be regarded as a black hole. When a normal node receives a Block message broadcasted by the IDS node, this node adds the malicious node which stored in the Block message into the Block table. After that, the normal node forwards RREP packet to establish the routing. If the RREP packet is acquired from its neighbor node which noted in the Block table, the normal node drops this RREP packet to prevent the malicious attack.

The proposed IDS scheme simulated under the existing one and two black holes network environment. The packet loss rate for AODV are 92.40% (one black hole) and 97.32% (two black hole), and 10.05% (threshold as 5) to 13.04% (threshold as 10) for IDS system with 9 IDS nodes. However, how to decide the threshold value does not be explained clearly in this paper.

4. Collaborative Black Hole Attack

There are various mechanisms have been proposed for solving single black hole attack in recent years. However, many detection schemes are failed in discussing the cooperative black hole problems. Some malicious nodes collaborate together in order to beguile the normal into their fabricated routing information, moreover, hide from the existing detection scheme. As a result, several cooperative detection schemes are proposed preventing the collaborative black hole attacks [35].

In the following, different detection schemes for the cooperative black hole attack are presented in a chronological order. The comparison of different schemes is shown in the Table 5.

Table 3 SN table

Node ID	Suspicious value	Status
3	1	Inactive
4	6	Active

Table 4 Block table

IDS node	Malicious node	Time
IDS_A	1	2009/02/19 12:51
IDS_C	6	2009/02/19 12:55

4.1. DRI Table and Cross Checking Scheme [36,37]

Sanjay Ramaswamy *et al.* exploit data routing information (DRI) table and cross checking method to identify the cooperative black hole nodes, and utilize modified AODV routing protocol to achieve this methodology.

Every node needs to maintain an extra DRI table, 1 represents for *true* and 0 for *false*. The entry is composed of two bits, "From" and "Through" which stands for information on routing data packet from the node and through the node respectively. As shown in Table 6, the entry 1 1 implies that node 1 has successfully routed data packets from or through node 5, and the entry of 0 0 means that node 1 has not routed any data packets from or through node 3.

The procedure of proposed solution is simply described as below. The source node (SN) sends RREQ to each node, and sends packets to the node which replies the RREP packet. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross checks its own table and the received DRI table to determine the IN's honesty. After that, SN sends the further request to IN's NHN for asking its routing information, including the current NHN, the NHN's DRI table and its own DRI table. Finally, the SN compares the above information by cross checking to judge the malicious nodes in the routing path.

Authors propose a detection method to overcome the multiple black hole problems and the collaborative attacks, and submit the simulation result in [37]. The experiment result shows that this solution performs an almost 50% better than other solutions.

Table 5 Comparison of Collaborative Black Hole Attack Detection Schemes

Schemes	Routing protocol	Simulator	Publication year	Results	Defects
DRI and cross checking [36]	AODV	No simulator	2003	No simulation results	-
DRI table and cross checking using FREQ and FREP [37]	AODV	-	2007	A higher throughput performance almost 50% than AODV	5-8% more communication overhead of route request
DCM [38]	AODV	NS-2	2007	The PDR is improved from 64.14 to 92.93%, and the detection rate is higher than 98%	A higher control overhead than AODV
Hash based [39] Hashed-based	DSR	-	2009	No simulation results	-
MAC and Hash-based PRF Scheme [40]	AODV	NS-2	2009	The PDR is higher than 90% when AODV is inaccessible 50%	The malicious node is able to forge a fake reply to dodge the detection scheme
BBN and RIP [41]	AODV	-	2010	No simulation results	-
BDSR [43]	DSR	QualNET	2011	The PDR of BDSR is always higher than 90%	The overhead is minimal higher than DSR, but lower than WD approach

-: means unmentioned

Table 6 An additional table example of node 1

Node ID	Data Routing Information	
	From	Through
3	0	0
5	1	1

However, it wastes 5 to 8% communication overhead, and slightly increases the packet loss percentage because of the secure route discovery delay.

4.2. Distributed Cooperative Mechanism (DCM) [38]

Chang Wu Yu *et al.* propose a distributed and cooperative mechanism viz. DCM to solve the collaborative black hole attacks. Because the nodes works cooperatively, they can analyze, detect, mitigate multiple black hole attacks. The DCM is composed of four sub-modules which shown as Figure 2.

In the local data collection phase, an estimation table is constructed and maintained by each node in the network. Each node evaluates the information of overhearing packets to determine whether there is any malicious node. If there is one suspicious node, the detect node initiates the local detection phase to recognize whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If the inspection value is positive, the questionable node is regarded as a normal node. Otherwise the initial detection node starts the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbors to participate in the decision making. Because the notify mode utilizes broadcasting method, the network traffic is increased. A constrained broadcasting algorithm is used to restrict the notification range within a fixed hop count. A threshold viz. *thr* represents the maximum hop count range of cooperative detection message. Finally, the global reaction phase is executed to set up a notification system, and sends warning messages to the whole network. There are reaction modes in global reaction phase. Though the first reaction mode notifies all nodes in the network, but might waste lots of communication overhead. Each node only concerns its own black hole list and arranges its transmission route in other mode, however it might be exploited by malicious nodes and needs more operation time.

In the simulation results, the notification delivery ratio is from 64.12 (*thr* as 1) to 92.93% (*thr* as 3) when using different threshold values. Compare with the popular

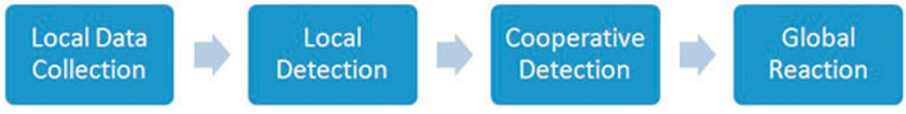

Figure 2 Working produces [38]. Figure 2 is working produces and the four sub-modules of Distributed Cooperative Mechanism (DCM). In the local data collection phase, an estimation table is constructed and maintained by each node in the network. Each node evaluates the information of overhearing packets to determine whether there is any malicious node. If there is one suspicious node, the detect node initiates the local detection phase to recognize whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If the inspection value is positive, the questionable node is regarded as a normal node. Otherwise the initial detection node starts the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbors to participate in the decision making. Finally, the global reaction phase is executed to set up a notification system, and sends warning messages to the whole network.

AODV routing protocol in MANET, the simulation result shows that DCM has a higher data delivery ratio and detection rate even if there are various black hole nodes. Even though the control overhead can be reduced due to the distributed design method, DCM wastes few overhead inevitably.

4.3. Hash based Scheme [39]

Weichao Wang *et al.* design a hash based defending method to generate node behavioral proofs which involve the data traffic information within the routing path. The developing mechanism is based on auditing technique for preventing collaborative packet drop attacks, such as collaborative black hole and grey hole problems. The proposed solution is originated from an audit-based detection method videlicet REAct [30], which is also discussed in the subsection 0 in this survey.

The vulnerability of REAct system is that cooperative adversaries can specialize in attacker identification phase by sharing Bloom filters of packets between them. The major difference between these two schemes is discussed as follows. A hash based node behavioral proofs is proposed to defend the collaborative attacks. The audited node n_i is needed and settled by the source node S, and then S sends the sequence numbers of selected packets to auditing node. After source node sends out these packets, an additional random number t_0 is attached to the tail of every packet. The intermediate node n_1 combines the received packet and its own random number r_1 to calculate its value t_1, and this operation is continued within every intermediate node until n_i receives the packet. Nevertheless, this paper doesn't give the results, so that it's hard to figure out the enhancement.

4.4. Hashed-based MAC and Hash-based PRF Scheme[40]

Zhao Min and Zhou Jiliu propose two hash-based authentication mechanisms, the message authentication code (MAC) and the pseudo random function (PRF). These two proposals are submitted to provide fast message verification and group identification, find the collaborative suspicious hole nodes and discover the secure routing path to prevent cooperative black hole attacks.

The public key infrastructure (PKI) is difficult to utilize in MANET due to the inherently design disadvantages, which is no centralized infrastructure. To deserve to be mentioned, authors overcome this bottleneck and design an authentication mechanism. The key point of this solution is that each node acquires a secret key K_i, and $K_i = G_k(r_i)$. The sharing key K_i is undisclosed to all other nodes, hence, it is formulated by choosing a random number r_i and repeatedly applying PRF on r_i by k times. When source node receives a packet, it checks $K_{i\text{-}d}$ to find whether the key used for the MAC is disclosed or not, and checks the MAC when K_i is disclosed. After checking the above two conditions, this packet is regarded as available packet and the route is confirmed as a secure route. On the other hand, authors propose the other solution based on time stamp method and global symmetric cryptosystem. However, we don't discuss this solution due to the time stamp method is well-known, and the global symmetric cryptosystem is designed based on accompanying the time delay range.

The simulation result shows that both solutions have better data delivery ratio than AODV routing protocol. But, the detection time increases as the pause time raises, and the control overhead of both solutions is higher than the ordinary AODV.

Moreover, the malicious node is able to forge the false reply packets and try to avoid the detection mechanism.

4.5. Backbone Nodes (BBN) and Restricted IP (RIP) Scheme [41]

Vishnu K. and Amos J. Paul address a mechanism to detect and remove the black and gray hole attack. This solution is able to find the collaborative malicious nodes which introduce massive packet drop percentage. An idea of the group of backbone nodes used in MANET was originated from [42]. Vishnu K. *et al.* refer this method to penetrate their system model, and also add a novel scheme videlicet restricted IP (RIP) to avoid collaborative black and gray attacks.

The detailed procedure is characterized as the following. In this solution initially a backbone network is established which constructed from a set of strong backbone nodes (BBNs) over the ad hoc network. These trusted nodes can be allowed to allocate the RIP when there is new arrival node joining. A node acquires a RIP which means that it is provided with the routing authority. The source node requests the nearest BBN to allot a RIP before transmitting data packets, then sending RREQ to the destination node and the address of RIP. If the source node only receives the destination node's RREP, it means that there is no black hole. In the case when the source obtains the RREP packet from RIP, it implies that adversary might be existed in the network. The RIP's neighbor nodes change to promiscuous mode as a result of the source node sends monitor messages to alert them. These neighborhoods not only monitor the packets of designate nodes but also the suspicious nodes. Furthermore, the source node sends few dummy data packets to test the malicious node. The neighbor nodes monitor the data packet flow and regard it as a black hole if the packet loss rate exceeds the normal threshold, and notify the source node that it is a malicious attacker. Then the neighbor nodes broadcast this alert message through the whole network, and add the malicious nodes to the black hole list. Finally, the attacker's authorization will be deleted and all of nodes drop the response from nodes in the black list.

The proposed solution not only detects black hole but also gray hole attacks, since its methodology does not utilize the trust-based method. However, it's hard to realize that how is the enhanced performance because there is no any simulation result or experiment outcome. Moreover, the proposed system might be crashed if the numbers of attackers are higher than the numbers of normal nodes.

4.6. Bait DSR (BDSR) based on Hybrid Routing Scheme [43]

Po-Chun Tsou *et al.* design a novel solution named Bait DSR (BDSR) scheme to prevent the collaborative black hole attacks. The proposed mechanism is composed of proactive and reactive method to form a hybrid routing protocol, and the major essence is the DSR on-demand routing. This solution is briefly introduced as below.

In the beginning of routing stage, the source node sends bait RREQ packet before starting route discovery. The target address of bait RREQ is random and non-existent. To avoid the bait RREQ inducing the traffic jam problem, BDSR use the same method with DSR. That is all bait RREQ packets only survive for a period time. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from black hole node. In authors' mechanism, the generator of RREP is recorded in the RREP's additional field. Therefore the source node can recognize the location of attacker from the reply location of RREP. All of the response sent

by the adversaries should be drop. After the initial phase, authors employ the original DSR route discovery procedure. If the data delivery rate is lower than the pre-defined threshold value, the bait procedure will be triggered again to examine the uncertainly suspicious nodes.

Compare with the primitive DSR scheme and watch dog method, the simulation results show that BDSR provides an excellent packet delivery rate. The packet delivery ratio of BDSR is 90% which is more superior to DSR and WD approach. Moreover, the communication overhead is also lower than watch dog scheme but slightly higher than original DSR routing protocol.

5. Conclusions and Future Works

Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem. In this paper, we first summary the pros and cons with popular routing protocol in wireless mobile ad hoc networks. Then, the state-of-the-art routing methods of existing solutions are categorized and discussed. The proposals are presented in a chronological order and divided into single black hole and collaborative black hole attack.

According to this work, we observe that both of proactive routing and reactive routing have specialized skills. The proactive detection method has the better packet delivery ratio and correct detection probability, but suffered from the higher routing overhead due to the periodically broadcast packets. The reactive detection method eliminates the routing overhead problem from the event-driven way, but suffered from some packet loss in the beginning of routing procedure. Therefore, we recommend that a hybrid detection method which combined the advantages of proactive routing with reactive routing is the tendency to future research direction. However, we also discover that the attacker's misbehavior action is the key factor. The attackers are able to avoid the detection mechanism, no matter what kinds of routing detection used. Accordingly, some key encryption methods or hash-based methods are exploited to solve this problem. The black hole problem is still an active research area. This paper will benefit more researchers to realize the current status rapidly.

List of abbreviations

Acronym: Definition; ABM: anti-black hole mechanism; AODV: ad hoc on-demand distance vector; BBN: backbone nodes; BDSR: bait DSR; BIT: black identification table; CRRT: collect route reply table; DCM: distributed cooperative mechanism; DDoS: distributed denial of service; DoS: denial of service; DPRAODV: detection, prevention and reactive AODV; DRI: data routing information; DSDV: destination sequenced distance vector; DSR: dynamic source routing; GloMoSim: global mobile simulator; IDS: intrusion detection system; IN: intermediate node; IT: isolation table; MAC: message authentication code; MANET: mobile ad hoc network; NHN: next hop node; OLSR: optimized link state routing; PDR: packet delivery ratio; PFC: packet forwarded count; PKI: public key infrastructure; PMC: packet modified count; PRC: packet received count; PRF: pseudo random function; REAct: resource efficient accountability; RIP: restricted IP; RREP: route reply; RREQ: route request; RRER: route error; SAODV: secure AODV; SN: source node; TORA: temporally-ordered routing algorithm; WD: watchdog; ZRP: zone routing protocol.

Acknowledgements

The authors would like to thank Po-Chun Tsou for his valuable suggestions and guidance in preparing this manuscript. The authors would like to thank Yu-Yan Lin for her assistance in polishing the paper writing. The authors would like to thank the referees for their helpful comments in improving the contents of this paper.

Author details

[1]Department of Computer Science & Information Engineering, National Central University, Taiwan [2]Department of Electronic Engineering, National Ilan University, Taiwan [3]Institute of Computer Science & Information Engineering, National Ilan University, Taiwan [4]Department of Electrical Engineering, Naitonal Dong Hwa University, Hualien, Taiwan

Authors' contributions
F-HT carried out the survey work, analyzed all schemes and compared them, and drafted the manuscript. Both L-DC and H-CC carried out the supervision of the manuscript, participated in its design and coordination, and helped to draft the manuscript.
All authors read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Received: 16 October 2011 Accepted: 22 November 2011 Published: 22 November 2011

References
1. Burbank JL, Chimento PF, Haberman BK, Kasch WT (2009) Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology. IEEE Communication Magazine 44(11):39–45. doi: 10.1109/COM-M.2006.248156
2. Sarma N, Nandi S (2010) Service differentiation using priority-based MAC protocol in MANETs. International Journal of Internet Protocol Technology 5(3):115–131. doi: 10.1504/IJIPT.2010.035383
3. Ting H-C, Chang R-S (2003) Improving the Performance of Broadcasting in Ad Hoc Wireless Networks. Journal of Internet Technology 4(4):209–216
4. Liao W-H, Tseng Y-C, Lo K-L, Sheu J-P (2000) GeoGRID: A Geocasting Protocol for Mobile Ad Hoc Networks Based on GRID. Journal of Internet Technology 1(2):22–32
5. Yang S-J, Lin Y-C (2009) Static and Dynamic RED Tuning for TCP Performance on the Mobile Ad Hoc Networks. Journal of Internet Technology 10(1):13–21
6. Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF (2005) A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks. Paper presented at the IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan, 28-30 March 2005
7. Zhou L, Chao H-C (2011) Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network 25(3):29–34. doi: 10.1109/MNET.2011.5772059
8. Yang H, Lou H, Ye F, Lu S, Zhang L (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications 11(1):38–47. doi: 10.1109/MWC.2004.1269716
9. Umang S, Reddy BVR, Hoda MN (2010) Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption. IET Communications 4(17):2084–2094. doi: 10.1049/iet-com.2009.0616
10. Wu B, Chen J, Wu J, Cardei M (2007) A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Xiao Y, Shen X, Du D-Z (eds) Wireless Network Security. on Signals and Communication Technology. Springer, New York
11. Marti S, Giuli TJ, Lai K, Baker M (2000) Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. Paper presented at the 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, 6-11 August 2000
12. Tseng Y-C, Jiang J-R, Lee J-H (2004) Secure Bootstrapping and Routing in an IPv6-based Ad Hoc Network. Journal of Internet Technology 5(2):123–130
13. Hu Y-C, Perrig A (2004) Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy 2(3):28–39. doi: 10.1109/MSP.2004.1
14. Raja Mahmood RA, Khan AI (2007) A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks. Paper presented at the International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, 18-20 November 2007
15. Saini A, Kumar H (2010) Comparison between Various Black Hole Detection Techniques in MANET. Paper presented at the National Conference on Computational Instrumentation, Chandigarh, India, 19-20 March 2010
16. Murty MS, Das MV (2011) Performance Evaluation of MANET Routing Protocols using Reference Point Group Mobility and Random Waypoint Models. International Journal of Ad hoc, Sensor & Ubiquitous Computing 2(1):33–43. doi:10.1155/2008/860364
17. Royer EM, Toh C-K (1999) A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications 6(2):46–55. doi: 10.1109/98.760423
18. Sanzgiri K, Dahill B (2002) A Secure Routing Protocol for Ad Hoc Networks. Paper presented at the 10th International Conference on Network Protocols, Paris, France, 12-15 November 2002
19. Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Paper presented at the ACM SIGCOMM'94 Conference, London, United Kingdom, August 31 - September 2, 1994
20. Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L (2001) Optimized Link State Routing Protocol for Ad Hoc Networks. Paper presented at the IEEE International Multi Topic Conference, Lahore, Pakistan, 28-30 December 2001
21. Perkins CE, Royer EM (1999) Ad-hoc On-Demand Distance Vector Routing. Paper presented at the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, Louisiana, 25-26 February 1999
22. Johnson DB, Maltz DA (1996) Dynamic Source Routing in Ad Hoc Wireless Networks. In: Imielinski T, Korth H (eds) Mobile Computing, vol 353. Kluwer Academic Publishers, pp 153–181
23. Haas ZJ, Pearlman MR, Samar P (2002) The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft
24. Park V, Corson S (1998) Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification. Internet Draft, Internet Engineering Task Force MANET Working Group
25. Deng H, Li W, Agrawal DP (2002) Routing Security in Wireless Ad-hoc Networks. IEEE Communications Magazine 40(10):70–75. doi: 10.1109/MCOM.2002.1039859
26. Sun B, Guan Y, Chen J, Pooch UW (2003) Detecting Black-hole Attack in Mobile Ad Hoc Networks. Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003

27. Al-Shurman M, Yoo S-M, Park S (2004) Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004
28. Tamilselvan L, Sankaranarayanan V (2007) Prevention of Blackhole Attack in MANET. Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007
29. Djenouri D, Badache N (2008) Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6
30. Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits. Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009
31. Raj PN, Swadas PB (2009) DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET. International Journal of Computer Science 2:54–59. doi: abs/0909.2371
32. Jaisankar N, Saravanan R, Swamy KD (2010) A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26-27 March 2010
33. Mistry N, Jinwala DC, IAENG, Zaveri M (2010) Improving AODV Protocol Against Blackhole Attacks. Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010
34. Su M-Y (2011) Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications 34(1):107–117. doi:10.1016/j.comcom.2010.08.007
35. Oliveira R, Bhargava B, Azarmi M, Ferreira EWT, Wang W, Lindermann M (2009) Developing Attack Defense Ideas for Ad Hoc Wireless Networks. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009
36. Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K (2003) Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003
37. Weerasinghe H, Fu H (2007) Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007
38. Yu CW, Wu T-K, Cheng RH, Chang SC (2007) A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network. Paper presented at the PAKDD workshops, Nanjing, China, 22-25 May 2007
39. Wang W, Bhargava B, Linderman M (2009) Defending against Collaborative Packet Drop Attacks on MANETs. Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009
40. Min Z, Jiliu Z (2009) Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks. Paper presented at the International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 16-17 May 2009
41. Vishnu KA, Paul J (2010) Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Networks. International Journal of Computer Applications 1(22):38–42. doi: 10.5120/445-679
42. Agrawal P, Ghosh RK, Das SK (2008) Cooperative Black and Gray Hole Attacks in Mobile Ad hoc Networks. Paper presented at the 2nd International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, January 31-February 01, 2008
43. Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L (2011) Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs. Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011

doi:10.1186/2192-1962-1-4
Cite this article as: Tseng *et al.*: **A survey of black hole attacks in wireless mobile ad hoc networks.** *Human-centric Computing and Information Sciences* 2011 **1**:4.