J Inf Process Syst, Vol.14, No.1, pp.56~78, February 2018
https://doi.org/10.3745/JIPS.03.0090

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Black Hole along with Other Attacks in MANETs: A Survey

Fan-Hsun Tseng*, Hua-Pei Chiang**, and Han-Chieh Chao***

Abstract

Security issue in mobile ad hoc network (MANET) is a promising research. In 2011, we had accomplished a survey of black hole attacks in MANETs. However network technology is changing with each passing day, a vast number of novel schemes and papers have been proposed and published in recent years. In this paper, we survey the literature on malicious attacks in MANETs published during past 5 years, especially the black hole attack. Black hole attacks are classified into non-cooperative and collaborative black hole attacks. Except black hole attacks, other attacks in MANET are also studied, e.g., wormhole and flooding attacks. In addition, we conceive the open issues and future trends of black hole detection and prevention in MANETs based on the survey results of this paper. We summarize these detection schemes with three systematic comparison tables of non-cooperative black hole, collaborative black hole and other attacks, respectively, for a comprehensive survey of attacks in MANETs.

Keywords

Collaborative Black Hole Attack, Flooding Attack, Mobile Ad Hoc Network, Non-cooperative Black Hole Attack, Wormhole Attack

1. Introduction

Ad hoc network [1] is a decentralized network type that distributed nodes communicate with each other without any pre-existing infrastructure. A great number of ad hoc applications have been proposed and investigated for many years, e.g., mobile ad hoc network (MANET) and vehicular ad hoc network (VANET). Through wireless medium, ad hoc nodes are movable, self-configured, self-organized, and are arbitrary to leave or join network. However, the non-infrastructure network architecture gives rise to critical security problems such as black hole, wormhole, flooding, and Sybil attacks. The detection of malicious attacks in ad hoc networks is vital and challenging [2].

A black hole attack means that one or multiple malicious nodes violate routing rules and drop all received packets. Malicious nodes are able to achieve their misbehaviors through many ways. It is often seen black hole attacks in MANETs [3]. An example of black hole node with forged route reply (RREP) packet is shown as Fig. 1. The source node is node 1 and the node 6 is destination node. The node 3 is a

Manuscript received October 30, 2017; first revision December 13, 2017; accepted December 26, 2017.
Corresponding Author: Han-Chieh Chao (hcc@mail.ndhu.edu.tw)
* Dept. of Technology Application and Human Resource Development, National Taiwan Normal University, Taipei, Taiwan (fanhsuntseng@ieee.org)
** Network and Technology Division, FarEasTone Telecommunications Co. Ltd., Taipei, Taiwan (vchiang@fareastone.com.tw)
*** Dept. of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan,; Dept. of Computer Science and Information Engineering, National Ilan University, Yilan, Taiwan (hcc@mail.ndhu.edu.tw)

malicious node that sends forged RREP packets. In the example, the source node sends route request (RREQ) to its neighbors as well as the node 2 and node 4 for establishing a path towards destination. The node 4 forwards the RREQ packet to node 5 then the node 5 forwards it to the destination node. After that, node 6 replies RREP packet and states that it is the destination node. However, on the other path, node 2 forwards the RREQ packet to node 3. In general, node 3 should forward the RREQ packet to node 6 for the establishment of routing path but it is a black hole node. The malicious node as well as node 3 sends forged RREP packet and claims that it has the shortest path to destination. Moreover, the node 3 drops the received RREQ packet sent by node 2 and does not forward it to destination. Network operation breaks down under the incorrect routing due to the malicious node 3. As a result, the network suffers from unsatisfying packet delivery ratio (PDR) caused by the attack from the black hole node.

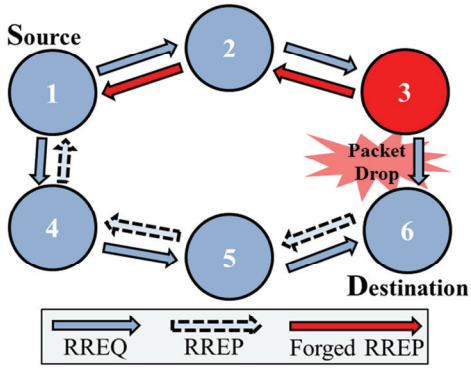

Fig. 1. A black hole attack based on forged route reply packet.

Although we had surveyed black hole attacks in MANETs and had published a survey paper [3] in 2011, a vast number of papers on black hole attacks detection and prevention have been published from 2012 to nowadays. In the paper, schemes for detecting and preventing black hole and other attacks in MANETs are studied. Note that we only survey the papers have been published in recent five years. We classify black hole attacks into non-cooperative and collaborative black hole attacks according to the attack behavior. The taxonomy of references in this survey is listed in Table 1.

Table 1. Taxonomy of references in this survey

Category	*References*
Non-cooperative black hole	[11], [12], [13], [14], [15], [16], [17], [18], [19], [21], [22], [23], [24], [25], [26], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [41], [49], [50]
Collaborative black hole	[20], [40], [42], [43], [44], [45], [46], [47], [48], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60]
Other attacks	[61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72]

The rest of the paper, as the roadmap depicted in 0 shows, is organized as follows. In Section 2, routing protocols in MANET are classified and introduced, i.e., reactive, proactive, and hybrid routing protocols. Section 3 surveys existing literature on non-cooperative black hole attack detection and prevention. Section 4 surveys existing literature on collaborative black hole attack detection and

prevention. Section 5 discusses other attacks in MANETs, e.g., intrusion, wormhole, flooding, and Sybil attacks. Section 6 discusses open issues of black hole attacks and the future trends. Finally, Section 7 concludes this survey.

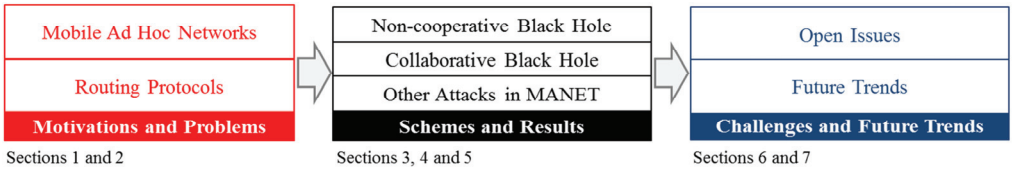

Fig. 2. Roadmap of this survey.

2. Routing Protocols

Before studying attacks in MANET, routing protocols [4] should be introduced. We classify routing protocols in MANET into three types according to their routing operation, i.e., proactive, reactive, and hybrid routing protocols.

The reactive routing protocol is also known as the on-demand routing protocol. Two most well-known reactive routing protocols are the ad hoc on-demand distance vector (AODV) [5] and the dynamic source routing (DSR) [6]. In a reactive routing protocol, mobile nodes update their routing information only when a node expects to transmit its data packets or its previous connection disconnected. Therefore the reactive routing protocol outperforms proactive routing protocol in terms of network throughput and routing overhead. However, the passive routing method leads to higher packet loss ratio with compared to the active routing method of proactive routing protocols. The difference between AODV and DSR is that DSR not only records next hop information but also maintains the route cache in routing table, which is different to the AODV records the next hop information only. According to this survey, we found that most of researchers apply reactive routing protocols such as AODV and DSR to their detection and prevention schemes. This is attributed to the reason that PDR is vital importance to the operation of MANETs.

The proactive routing protocol is also known as the table-driven routing protocol. Two well-known proactive routing protocols are the destination sequenced distance vector (DSDV) [7] and the optimized link state routing (OLSR) [8] protocols. In a proactive routing protocol, mobile nodes broadcast routing information periodically that results in higher routing overhead. When network scale increases, the routing overhead raises due to more routing information from more mobile nodes. A node with proactive routing protocol needs to maintain its routing table once network topology changes. The routing table of a node records its neighbor information, such as adjacent nodes and reachable nodes. When a node leaves or joins the network, each node updates its routing table so that black hole detection and prevention can be more instantaneous.

The hybrid routing protocol integrates reactive and proactive routing protocols into a new routing method. Two familiar hybrid routing protocols are the temporally-ordered routing algorithm (TORA) [9] and the zone routing protocol (ZRP) [10]. A hybrid routing protocol starts with proactive routing method that collects routing information in routing table, and updates routing table with reactive routing method when network topology changes.

3. Non-cooperative Black Hole Attack Detection and Prevention

A non-cooperative black hole attack means that a malicious node forges false information to accomplish its misbehavior without cooperating with other malicious nodes. For example, a malicious node is able to declare it has the shortest path to destination node so that other nodes mistransmit packets to the malicious node. However the malicious node drops these packets as well as a black hole attack and transmits fake routing packets to destroy regular routing operation. The comparison of existing literature on non-cooperative black hole attack in MANET is captured in Table 2.

Table 2. The detection schemes for non-cooperative black hole attack in MANET

Scheme	*Routing protocol*	*Publication year*	*Simulator*	*Result*	*Defect*
Agent-based AODV [11]	AODV	2012	NS-2 (v. 2.34)	Improve PDR to 99%, decrease NRL to 0.01, improve 10% end-to-end delay than AODV	Failed when attackers cooperate to forge fake reply packets and false flags
Sharma and Sharma [12]	AODV	2012	NS-2	Simulation results are the same with the results in [13]	The idea was proposed by [13] in 2004 and results are the same
OAODV [14]	AODV	2012	NS-2 (v. 2.34)	Achieve 78.65% PDR of AODV	May be failed when destination node is an attacker or multiple malicious nodes
Trust based AODV [15]	AODV	2012	NS-2	Maintain 60% to 90% PDR when there are 20 attackers	Failed when attackers cooperate to forge fake RREP packets
AODV-IDPS [18]	AODV	2012	NS-2	Detect black hole attack by analyzing trace files	Cannot eliminate black hole in time and cannot prevent attacks
Singh and Sharma [19]	AODV	2012	QualNet 5.0.1	Reach 90% throughput but increase 0.04 end-to-end delay	The concept of promiscuous mode was proposed in [18]
Jaiswal and Kumar [21]	AODV	2012	NS-2	Higher PDR and larger end-to-end delay with compared to AODV	Usage of destination sequence number and RRT were proposed in [20,21]
GA based IDS [24]	AODV	2012	NS-2 & MATLAB	Black hole nodes can be detected	Methodology of GA based IDS is unclear
ACO system [28]	-	2012	-	-	No experiment or simulation result
Adaptive method [29]	-	2012	-	-	No experiment or simulation result
DBA-DSR [30]	DSR	2013	GloMoSim	Higher PDR than DSR under different node mobility and number of malicious nodes	Network and routing overhead might be increased due to extra RREP packets

Table 2. (Continued)

Scheme	*Routing protocol*	*Publication year*	*Simulator*	*Result*	*Defect*
MDSR [31]	DSR	2013	GloMoSim	Compared to DSR, reduce 64% packet drop ratio but increase 8% control packet overhead	Assumptions are too optimistic to be applied to actual scenario
SVM [33]	AODV	2013	NS-3 (v. 3.14)	Discover more malicious nodes than previous method	Explanations of SVM-based method and the summation results are unclear
SRD-AODV [34]	AODV	2013	NS-2	85% PDR higher than standard AODV	Failed when attackers cooperate to forge false sequence number
Trust value [16]	AODV	2013	OMNeT ++	Higher threshold value leads to lower average packet loss	Failed when attackers cooperate to send fake RREQ and RREP packets
Trust model [17]	AODV	2014	-	Higher throughput and PDR, lower packet drop ratio	Explanation of experiments is unclear
SDRP [35]	AODV	2014	NS-2 (v. 2.34)	Slightly lower PDR with compared to AODV	Slightly higher routing overhead and latency
Watchdog [36]	AODV	2014	NS-2 (v. 2.34)	Slightly higher PDR, lower MAC load and end-to-end delay	Fail to detect multiple black hole nodes and collaborative attackers
Intrusion detection [32]	AODV	2015	NS-2 (v. 2.34)	Higher PDR, lower MAC load and end-to-end delay than AODV	The same defect with [26] that assumptions are too optimistic
IDSNAODV [37]	AODV	2015	NS-2	Higher throughput & PDR, lower packet loss rate & end-to-end delay	Failed in collaborative attack, rules of attacker identification is rough
Knowledge table [38]	AODV	2015	NS-2 (v. 2.35)	Higher PDR than standard AODV	Failed when attackers cooperate to forge their knowledge table
Fuzzy and GA [25]	AODV	2016	MATLAB	Throughput, PDR and error rate are estimated	Methodology of GA and fuzzy is unclear
IBFOA [26]	AODV	2016	MATLAB	Result of attackers prevention is unclear	Methodology of IBFOA is unclear
HSA [39]	DSR	2016	MATLA B 2015a	Higher throughput and PDR, lower routing overhead and end-to-end delay than CBDS	Hello message has been used in [52] already for identifying neighbors
STAODV [41]	AODV	2017	NS-2 (v. 2.35)	Higher throughput and PDR, and lower routing overhead than AODV	Failed when attackers cooperate to forge fake sequence number

The symbol "-" means unmentioned.

PDR=Packet Delivery Ratio, NRL=Network Routing Load, AODV-IDPS=Ad-hoc On-demand Distance Vector with Intrusion Detection and Prevention System, OAODV=Opinion AODV, RREP=Route Replay Packet, AODV-IDPS=Ad-hoc On-demand Distance Vector with Intrusion Detection and Prevention System, RRT=Route Reply Table, DSR=Dynamic Source Routing, MDSR=Modified DSR, SVM=Support Vector Machine, SRD-AODV=Secure Route Discovery AODV, SDRP=Secure Dynamic Routing Protocol, GA=Genetic Algorithm, IBFOA=Improved Bacteria Foraging Optimization Algorithm, HSA=Harmony Search Algorithm, CBDS=Cooperative Bait Detection Scheme, STAODV=Secure and Trust AODV.

In [11], the authors proposed an agent-based AODV routing method to detect and prevent black hole attack. The proposed method is simple that only modifies two functions of standard AODV. The first modification is *sendReply()* function and the other one is *recvReply()* function. The *sendReply()* function accommodates flag RREP packets and the *recvReply()* function is used to detect malicious nodes. If a received packet records that the node is destination and it is not set, the agent judges the node is a malicious node that pretends it is the destination node. Therefore, the agent discards the received RREP packet which is generated by the malicious node, and removes the malicious node from routing path. Another situation if a received packet records that a node is an intermediate hop and has route but its flag is set, the agent judges the node is a malicious node that claims it has the shortest route. Thereby the agent discards the RREP packet and eliminates the node from route. Simulation-based results showed that the proposed agent-based method increases PDR to 99%, minimizes network routing load to 0.01, and improves 10% end-to-end delay in average with compared to the standard AODV routing protocol. However, the proposed agent method detects malicious nodes by examining the flag in *sendReply()* function. It will be failed when malicious nodes cooperate to forge fake reply packets and false flags.

In [12], the authors proposed two possible solutions to solve black hole attack. The first one is to find more than one route to destination and the other one is to exploit the packet sequence number in packet header. However, these two solutions were proposed by Al-Shurman et al. [13] in 2004. They proposed the idea of redundant route method and unique sequence number scheme to identify a malicious node. In the unique sequence number scheme, two values are recorded in two extra tables when any packet is transmitted or received. Based on the comparison of current and updated sequence numbers, malicious nodes can be found easily. On the other hand, the simulation results in [12] are completely the same with the results in [13].

In [14], the authors proposed the opinion AODV (OAODV) to detect malicious node by comparing the number of route request with the number of router reply. Two additional fields are used in the OAODV, i.e., request weight and reply weight. The request weight records the number of RREQ packets forwarded and the reply weight registers the number of RREP packets forwarded. In addition, two control packets are newly proposed, i.e., opinion request (OREQ) and opinion relay (OREP) packets. Source node broadcasts OREQ packets and receives OREP packets from intermediate nodes except destination node, and then calculates the ratio of request weight to reply weight on each path. The malicious node can be discovered if the calculation result as well as the weight ratio is very small. Simulation results showed that the OAODV achieves 78.65% PDR of standard AODV without attacks and yields better PDR than of the AODV protocol under black hole attack. However the OAODV may be failed when the destination node is an attacker. Besides, it may be compromised if several malicious nodes cooperate to send forged OREP packets or to provide false number of OREP packets. Last, the routing overhead might be increased so that should be estimated.

In [15], the authors proposed a trust based collaborative approach for detecting malicious node under AODV protocol in MANET. In the approach, every node calculates the trust value on its neighbor nodes and monitors the trust value. The trust value is a ratio of dropped packets to forwarded packets so that it ranges 0 to 1. A malicious node is detected when its trust value is lower than the predefined threshold value, i.e., 0.3 as well as 30% forwarded packets are dropped. After that, the node is monitored by its neighbors and marked as a malicious node, thus eliminated from routing path. Simulation-based results showed that the modified AODV protocol keeps 60% to 90% PDR when there are 20 malicious

nodes. However, the approach will be failed when neighbor nodes cooperate to forge trust value. Attackers are capable of replying fake RREP to monitoring nodes, thereby the trust-based approach will be compromised. In 2013, Bar et al. [16] also used trust value to detect black hole attacks. The trust value of an intermediate node is obtained from two values, i.e., threshold value and weight factor. The threshold value (W_1) is defined as the number of transmitted packet divided by number of received packet. The weight factor (W_2) is defined as the number of transmitted RREP divided by number of received RREQ. After that, the trust value is calculated as $\text{Trust value} = W_1 * W_2 * \text{ptrust}$. However the authors did not explain what the variable ptrust is and how to obtain it. The authors utilized OMNeT++ to implement the simulation. Results showed that a higher threshold value leads to the lower average packet loss. However the proposed method will be failed if collaborative black hole nodes send fake RREQ and RREP packets. In 2014, Biswas et al. [17] also proposed a trust model to detect black hole attacks. In the proposed trust model, three parameters of each node are assigned and evaluated, i.e., rank, remaining battery power and stability factor. Experimental results showed that the proposed method yields higher PDR, throughput, and lower packet drop ratio with compared to previous methods. Black hole detection by trust value model has been investigated for many years, the concept of these papers are similar only different from evaluation metrics.

In [18], the authors proposed an ad-hoc on-demand distance vector with intrusion detection and prevention system (AODV-IDPS) to tackle with black hole attack. The AODV-IDPS module observes black hole attack and analyzes regular network's behavior. Based on the observation and analysis of routing overhead, average delay, throughput and PDR, the AODV-IDPS module compares the performance of regular network with current performance to execute intrusion detection. The proposed AODV-IDPS module detects black hole attack by analyzing trace files when a node creates network loop. However the proposed module cannot eliminate black hole attacks in real-time because it needs time to analyze and compare network performance from trace files. In other words, the detection and prevention is not simultaneous while a malicious node is launching.

In [19], the authors proposed a solution to black hole attack, which uses promiscuous mode to intercept and read network packets. In the promiscuous mode, a node can overhear other nodes once it is within the communication range of other nodes, even if the node does not directly communicate with other nodes. For instance, node A sends an RREP packet to node B, at that time, node C switches to promiscuous mode and sends a Hello message to node B through node A. If node A does not forward the reply packet from node B to node C, the node A is regarded as a malicious node. After that, node C floods an alarm message to all nodes in MANET that node A is a black hole and should be isolated from routing path. Simulation results showed that the proposed method performs a similar throughput to the standard AODV without black hole attack. On the other hand, the proposed method only increases 0.04 second in average end-to-end delay with compared to the AODV without black hole attack. However, the concept of promiscuous mode was proposed by Vishnu and Paul [18] in 2010. In [20], the restricted IP's neighbors change to promiscuous mode for monitoring the packets of designate node and suspicious nodes.

In [21], the authors proposed the *ReceiveReply* method based on destination sequence number, viz. RREP method. The RREP method examines the difference between the sequence number of source node or intermediate node who has sent RREP packet back or not. The destination sequence number is recorded in the route reply table. Simulation results showed that the proposed method yields higher PDR than AODV protocol but leads to larger end-to-end delay. However, we deem that the concept of

using destination sequence number to detect malicious nodes was proposed by [22] in 2010. On the other hand, the idea of checking sequence number in route reply table was proposed by [23] in 2007. In [23], packet's sequence number and received time are stored in a collected route reply table.

In [24], the authors utilized genetic algorithm (GA) to develop an intrusion detection system (IDS) for black hole attack in MANET. The proposed GA based IDS analyzes each node's behavior and detects black hole nodes according to the consideration of network parameters, e.g., packet drop, request forwarding rate and request receive rate. However, GA needs time for evolution that may not be suitable for detecting malicious nodes in MANET because the nodes move frequently and rapidly. In [25], the authors implemented fuzzy and GA with AODV protocol to prevent black hole attacks in VANET. However, the authors did not explain the implementation of proposed fuzzy and GA in the paper. In addition, the authors did not compare the proposed method with other existing schemes. In [26], the authors claimed that an improved bacteria foraging optimization algorithm (IBFOA) is proposed to prevent black hole attacks in MANET. The paper presents the enhanced AODV routing protocol [13] and the concept of bacterial foraging [27]. However the authors did not clarify how to combine the bacterial foraging method with the enhanced AODV. In addition, it cannot be observed that how the proposed method prevent hole attacks in the simulation results.

In [28], the authors proposed a concept of using ant colony optimization (ACO) system to detect black hole attack. The proposed ACO system is described as follows. Firstly, a start node is selected randomly. The trail of a path represents its selection possibility. A path with higher trail means that the path has higher selection probability. Ants continue selecting path until they reach the starting node. A finished tour in consequence is a solution of optimization. The higher probability of a selecting path will be part of a better solution. The ACO system repeats these steps until most ants select the same tour. However the explanation of the ACO system is unclear. For example, the formulation of pheromone calculation was missed in the paper. Besides, there is no experiment or simulation result.

In [29], the authors proposed the concept of an adaptive method of detecting black and grey hole attacks. In the paper, the authors claimed that extra control packet is unnecessary. They proposed a collision report mechanism to dynamically modify threshold according to the status of network loading. However the authors did not verify the proposed method with any convincing result.

In [30], the authors proposed a method of detecting black hole attack based on DSR, viz. DBA-DSR scheme. By sending fake RREQ packets, the DBA-DSR detects black hole nodes before actual routing process. It modifies DSR's RREP packet to retrieve the address of initiator RREP packet, because normal nodes should not reply the fake RREQ packet. The DBA-DSR identifies malicious nodes by examining the RREP initiator address. Simulation results showed that the DBA-DSR yields higher PDR than that of the DSR with varying node mobility and numbers of malicious nodes. However the network and routing overhead of DBA-DSR might be slightly increased due to extra fake RREQ packets.

In [31], the authors proposed an IDS to detect abnormal difference in the number of data packets forwarded by a node. In the system, source node divides data into different blocks and separately sends them once a data block. It eliminates network and routing overhead before transmitting actual data packets. Once an attack is detected, the IDS nodes switch to promiscuous mode. When a black or grey hole attack is detected, source node sends query request (QREQ) packets to a nodes where within 2-hop distance and then receives query reply (QREP) packets. If data packet forwarded count does not match,

the node sends QREP packet and its next hop node is moved to the suspected list. As a result, malicious nodes can be isolated from other nodes. Results showed that the proposed IDS reduces 64% packet drop ratio but raises 8% control packet overhead with compared to DSR under attack. However the assumptions of the work are too optimistic to be convincible. The authors assume that all nodes are authorized nodes which means that malicious node does not exist at the beginning. On the other hand, they also assume that source node and destination node are trusted nodes by default. In other words, malicious nodes exist in the intermediate nodes from source to destination only. After two years in 2015, Kumar and Dutta [32] proposed a similar intrusion detection technique to tackle with black hole attacks. The assumptions in [32] are almost the same with assumptions in [31]. In other words, the assumptions still limit malicious node exists in intermediate nodes only. As a result, the method will be compromised if the source node is an attacker.

In [33], the authors utilized support vector machine (SVM) to detect black hole attacks under AODV protocol in MANET. The proposed SVM-based method classifies the nature of nodes by three performance metrics, i.e., PDR, packet modification rate and packet misroute rate. These metrics are calculated based on numbers of transmitted, modified and misrouted packets respectively. Results showed that the SVM-based method performs better result than previous method. It is novel to utilize a learning-based method to detect attacks in MANET. However the explanation of proposed SVM is unclear. Besides the simulation results are unclear. It only can be observed that the SVM-based method detects more malicious nodes than previous method but without clear explanation.

In [34], the authors proposed a mechanism named secure route discovery AODV (SRD-AODV) to prevent black hole attacks. In the SRD-AODV, source node and destination node verifies the sequence numbers in RREQ and RREP packet respectively. The verification of destination sequence number is based on three predefined thresholds, i.e., small, medium and large environments. The calculations of three thresholds are similar to each other only with different constants. The source node will receive two RREP packets once there is a malicious node in network. If the destination sequence number in an RREP packet is greater than the predefined threshold, the RREP packet will be regarded as a fake packet sent by a black hole node. Results showed that the SRD-AODV yields higher PDR 85% at least with compared to standard AODV protocol no matter in small, medium or large environments. However the method might be failed when various attackers cooperate to forge false sequence numbers.

In [35], the authors proposed a secure dynamic routing protocol (SDRP) to prevent attacks, e.g., modification attack, black hole attack and wormhole attack. The SDRP maintains three secure parts, which are neighbor maintenance, route discovery and route maintenance. It not only generates a secret shared key between source node and destination node but also reduces number of signatures. With secure neighbor maintenance, a signed Hello message is sent to neighbors periodically to ensure no malicious node. With secure route discovery, random number and sequence number are used to guard routing path from source to destination. With secure route maintenance, when a node detects disconnection it sends a router error (RRER) message with signature to the source node. Simulation results showed that the proposed SDRP achieves 90% PDR which is slightly lower than standard AODV. However, the SDRP also results in higher routing overhead and latency with compared to AODV protocol.

In [36], the authors implemented a watchdog mechanism, viz. watchdog-AODV (W-AODV) to detect black hole node. The W-AODV is implemented in a node that monitors all nodes within its

transmission range. If a node is unwilling to forward packets to its neighbors or a forwarded packet is altered by its neighbors, the watchdog recognizes it as a malicious node and declares to all nodes. Simulation results showed that the W-AODV performs slightly higher PDR, lower MAC load and end-to-end delay with compared to standard AODV protocol. However the W-AODV mechanism is incapable of detecting collaborative black hole attacks even two malicious nodes without cooperation.

In [37], the authors proposed a new algorithm viz. intrusion detection system new AODV (IDSNAODV). The IDSNAODV identifies malicious nodes based on their behavior and then deletes them from route. The authors define some rules to identify malicious nodes. For instance, a node which has the smallest number of hops in RREP or has the highest number of sequences may be a malicious node, or the node receives many packets but only sends one packet may be an attacker. A node is regarded as a malicious node if the node receives some packets but does not send them to neighbors. Simulation results showed that the IDSNAODV outperforms the standard AODV in higher PDR, throughput and lower end-to-end delay. However the defined rules of identifying malicious nodes are not sophisticated. The reliability of detecting malicious nodes might be low and inaccurate.

In38, the authors proposed a secure knowledge algorithm with considering packet drop reasons. An extra knowledge table is established in each node to record the information of packets, which is most recently transmitted. In promiscuous mode, each node monitors the packets forwarded by its neighbors then compares neighbor information with the information stored in its knowledge table. If the information is different, then the node waits a specific time and checks the reason of packet dropping. The knowledge table is composed of two fields, i.e., *fm* and *rm* fields, where *fm* maintains recent forwarded packets and *rm* maintains the information of neighbor nodes' recent packets. Once *fm* is unequal to *rm* and packet drop reaches a predefined threshold, the node is recognized as a malicious node. Simulation results showed that the proposed method yields higher PDR than standard AODV under different number of malicious nodes. However the proposed method will be failed when attackers cooperate to forge knowledge table.

In [39], the authors proposed a harmony search algorithm (HSA) based on the modification of the cooperative bait detection scheme (CBDS) proposed by Chang et al. [40]. The major object is to reduce the delay in detecting malicious nodes. Fahad and Muniyandi [39] claimed that CBDS might misdirect the source node because DSR may provide no information to distinguish malicious nodes (false RREP message) from normal nodes (true route reply). Therefore a HELLO message is added to the CBDS for identifying true neighbor nodes. The HELLO message traverses subsequent nodes in the range of one hop. However, in the second paragraph of Section III in [40], they stated "To resolve this issue, the function of HELLO message is added to the CBDS to help each node in identifying which nodes are their adjacent nodes within one hop." Nevertheless, Fahad and Muniyandi [39] present that the HSA not only reduces lower routing overhead and end-to-end delay but also improves PDR and throughput with compared to CBDS and DSR in simulation results.

In [41], the authors proposed a secure and trust AODV (STAODV) to mitigate black hole attacks in MANET. In STAODV, each node has a trust value and a malicious node table. Every incoming packet has a safety value, which is used to examine its safety status. A threshold value is predefined to determine the reply is safe or not. The STAODV examines each RREP packet with the sequence number and the hop count of a node to destination, and also examines the safety status of route reply. The detection method by using sequence number has been proposed in many papers. The STAODV will be failed when attackers cooperate to forge fake sequence number in route reply message.

4. Collaborative Black Hole Attack Detection and Prevention

Table 3. The detection schemes for collaborative black hole attack in MANET

Scheme	*Routing protocol*	*Publication year*	*Simulator*	*Result*	*Defect*
Algorithmic approach [42]	AODV	2011	NS-2	-	PDR and throughput are analyzed in simulation but without approach implementation
Modified AODV [45]	AODV	2012	-	-	No simulation or experiment result
DCBA [46]	DSR	2012	QualNet	Higher throughput and less packet loss rate than BDSR [47]	Slightly higher end-to-end delay
EDRI [51]	AODV	2012	-	-	Failed when attackers cooperate to forge fake data routing information
GAODV [53]	AODV	2013	GloMoSim	Higher data delivery ratio than AODV	Higher end-to-end delay than AODV
Advanced DRI [52]	AODV	2013	NS-2	Higher throughput and PDR, and lower end-to-end latency than AODV	RREP table and DRI table are referred to [20] and [43]
Hash [54]	AODV	2014	NS-2	Higher PDR, throughput and lower end-to-end delay than AODV	The computation load of source and destination node might be high
Dynamic CBDS [40]	DSR	2015	QualNet 4.5	Higher PDR than DSR, 2ACK, and BFTR	Slightly higher routing overhead than DSR
ESCS [55]	DSR	2015	NS-2	Higher throughput and PDR with compared to SCS and DSR	Higher routing overhead and end-to-end delay
Trusted AODV [56]	AODV	2015	NS-2	Higher throughput, PDR, and remaining energy	Failed when attackers send false packets result in incorrect trust value
D-MBH and D-CBH [57]	AODV	2016	-	Less routing overhead and computational overhead	Only analysis without experiment or simulation
Prevention AODV [58]	AODV	2016	NS-2	Decrease 70% end-to-end delay, increase 45% PDR & 10% throughput	The methodology is similar to [57]
PPP [59]	-	2017	-	Larger network needs more placebo packets	Failed in a higher proportion of normal nodes to malicious nodes
CRCMD&R [60]	AODV	2017	MATLAB	Higher total throughput than standard AODV	Methodology is old except cluster technique

The symbol "-" means unmentioned.
ESCS=Enhanced Self-Checking Scheme, SCS=Self-Checking Scheme, DCBA=Detecting Collaborative Blackhole Attacks, BDSR=Bait DSR, CBDS=Cooperative Bait Detection Scheme, EDRI=Extended Data Routing Information, BFTR=Best-effort Fault-Tolerant Routing, GAODV=Gratuitous AODV, D-MBH=Detection of Multiple Black Hole, D-CBH=Detection of Collaborative Black Hole, PPP=Placebo Packet Protocol, CRCMD&R=Cluster and Reputation based Cooperative Malicious node Detection and Removal.

A collaborative black hole attack coordinates several malicious nodes cooperate to forge fake packets for reaching their misbehavior. For example, a fake RREQ or RREP sent by single attacker may be detected due to the inconsistent information of hop count or sequence number. However, two or more attackers are able to collaborate with each other for deceiving above-mentioned detection schemes. In recent years, various schemes for collaborative black hole detection have been published. The comparison of literature on cooperation schemes is captured in Table 3.

In [42], the authors proposed an 'algorithmic approach' for improving the security of AODV. An additional route is proposed to request the identity of intermediate node to the node in next hop. Two main functions are used in the paper, i.e., data routing information (DRI) table and cross checking. However, the DPI table and cross checking method were proposed by Ramaswamy et al. [43] in 2003 and Weerasinghe and Fu [44] in 2007. In [3], we have surveyed and introduced [43] and [44] clearly. The concept of DPI table and cross checking was proposed in [43] and verified with simulation in [44]. The simulation-based results showed that the proposed method in [44] yields a higher throughput performance around 50% than that of the standard AODV protocol, but increases 5% to 8% communication overhead of route request. The process of the algorithmic approach in [42] is introduced as follows. First of all, source node broadcasts RREQ packets and receives RREP packets from other nodes. Then the source node receives the further request, next hop node and DRI entry for next hop's next hop. After that, the DPI entry is used to examine the intermediate node is a malicious node or not. However they did not verify the algorithmic approach in any experimental or simulation-based results. In the simulations of the paper, they discuss the effect of black hole attack in terms of PDR and throughput with varying node mobility.

In [45], the authors proposed a 'modified AODV protocol' and a 'watchdog mechanism' to detect black hole attack and wormhole attack. Two extra tables are maintained in each node, i.e., pending packet table and node rating table. The four fields of pending packet table are captured in Fig. 3 and the four fields of node rating table are captured in Fig. 4. The ID of packet sent, the address of next hop, the time-to-live of packet, and the address of destination node are filled in the pending packet table. In node rating table, the address of next hop, a counter for counting dropped packets, a counter for counting forwarded packets, and a tuple named misbehave are recorded. Note that the misbehave tuple is used to represent node behavior, i.e., 0 is well behaving node and 1 is misbehaving node. Based on the information in node rating table, the watchdog calculates the ratio of dropped packets to forwarded packets. All packets in MANET check any received packet to prevent false packets. If a data packet expires in the pending packet table, the packet drops field counts and deletes the data packet from pending packet table. If the calculation result is higher than a predefined threshold, the node is regarded as a malicious node and notes 1 in the misbehave field of node rating table. The proposed method is capable of detecting non-cooperative black hole attack even if two malicious nodes cooperate with each other to forge false packets. However, there is no simulation or experiment result to verify the proposed methodology.

Packet ID	Next Hop	Expiry Time	Packet Destination

Fig. 3. The four fields of pending packet table in [45].

Next Hop	Packet Drops	Packet Forwards	Misbehave

Fig. 4. The four fields of node rating table in [45].

In [46], the authors proposed the detecting collaborative blackhole attacks (DCBA) scheme based on the concept of the cooperative bait detection scheme (CBDS) [47]. In simulation results, the DCBA scheme yields higher network throughput and less packet loss percentage than that of the Bait DSR (BDSR) [48] scheme. Note that we have studied the BDSR scheme in our previous survey [3]. On the other hand, Chang et al. [40] improved CBDS by using a dynamic threshold. The improved CBDS scheme implements a reverse tracing technique to alarm source node to trigger detection scheme again. The advantages of proactive detection and reactive response are both utilized to achieve collaborative black hole detection. Results showed that the improved CBDS yields the highest PDR compared with DSR, 2ACK [49] and the best-effort fault-tolerant routing (BFTR) [50] protocols.

In [51], the authors proposed a mechanism to detect and remove cooperative blackhole and grayhole attacks by maintaining the extended data routing information (EDRI) table in each node. In EDRI table, it records the count of a malicious node been catching by other nodes. The identification of a malicious node depends on its catch count, which is proportional to time. If the node is being caught frequently it will be regarded as a malicious node then removed from routing path. However the paper did not present any experiment or simulation. In addition, we consider that the proposed mechanism will be failed when collaborative malicious nodes forge their DRI table. In [52], the authors deployed the advanced DRI table with a check bit to AODV protocol for detecting cooperative black hole attacks. A table of RREP message and a timer are used in the proposed solution. However the concept of RREP table and DRI table is referred to [22] and [44], respectively.

In [53], the authors proposed the gratuitous AODV (GAODV) algorithm by using the gratuitous RREP packet. The concept of the gratuitous RREP packet is addressed as follows. In AODV protocol, when an intermediate node has a route to destination node, it sends RREP packet to source node. Then, the GAODV scheme unicasts a gratuitous RREP packet to the destination node. The authors took advantage of the gratuitous RREP packet to detect malicious nodes by applying it as a CONFIRM packet. In GAODV protocol, source node unicasts the CHCKCFRM packet to destination node. The black hole node will be detected because it fails to send the CONFIRM packet so that the destination node never generate CHCKC packet. Note that an extra check table is needed to record the relay value of each node regarding the CHCKCFRM and CONFIRM packets. Simulation results showed that the GAODV protocol outperforms standard AODV in higher data delivery ratio but leads to longer end-to-end delay.

In [54], the authors utilized hash function to maintain data integrity for preventing black hole attack. When the destination node receives message, the hash value (SHA-TWO) of the message is computed. If hash values are the same between source node and destination node, the route is regarded as a secure route otherwise the destination node broadcasts data packet error message to source node. After that, the route is marked in routing table and will not be used any more. Simulation results showed the proposed method is superior to standard AODV in terms of higher PDR, throughput, and lower end-to-end delay.

In [55], the authors proposed a self-checking scheme (SCS) and an enhanced SCS (ESCS) to prevent

collaborative black hole nodes. The SCS is composed of three main steps that are update and maintain neighborhood topology, liar checking, and consistency checking. In the first step, the authors utilized Hello message exchange method [35] to accomplish neighborhood topology table maintenance. In lair checking step, a node executes liar checking before updating reports to its two-hop neighbors when it receives a Hello message. If a node cheats other nodes with false message that is asymmetric to the destination cache of other nodes, it will be listed into liar list and the lying-count increases. Once the lying-count is higher than a predefined threshold, the node will be put into the black list. In consistency checking step, each node executes consistency checking to make sure that received RREP message is consistent to neighborhood topology. The ESCS improves SCS by periodically sending Hello message to two-hop neighbors. As a result, collaborative black hole nodes can be found. Simulation results showed that the ESCS is superior to SCS in terms of higher PDR and throughput but increases routing overhead and end-to-end delay.

In [56], the authors proposed a trusted AODV to detect and avoid wormhole and collaborative black hole attacks. Nodes are classified into three types regarding the trust level, i.e., unreliable, reliable and most reliable. An extra trust table is maintained in each node to record the trust value of its neighbors. The trust value of a node is calculated as $T = \tanh(R1 + R2)$, where $tanh()$ is a hyperbolic tangent function. Variable $R1$ is the ratio of packets actually forwarded to packets to be forwarded, and variable $R2$ is the ratio of packets received from a node sent by others to total packets received. When an incoming node joins the network, its trust level is set to unreliable. Then three threshold values are defined to determine its trust level, which are T_{ur}, T_r and T_{mr}, Note that these threshold values are decided and set in simulation setting. Results showed that the trusted AODV provides higher PDR, throughput and remaining energy with compared to the wormhole AODV scheme. However, collaborative malicious nodes are capable of sending fake packets so that the trusted AODV will be compromised due to false trust value.

In [57], the authors proposed a strategy to detect malicious nodes in MANETs. To detect non-cooperative black hole attacks, the detection of multiple black hole (D-MBH) scheme is proposed to send a fake RREQ message to request an additional route with non-existent target address. The D-MBH scheme computes a threshold of average destination sequence number and creates a list of black hole nodes. The authors further proposed the detection of collaborative black hole (D-CBH) scheme. The difference between D-MBH and D-CBH is that the D-CBH scheme further extracts the next hop information from RREP. After that, the D-CBH also creates a list of collaborative black hole nodes. However, the paper only presents analysis result rather than simulation result. The analysis results showed that the proposed scheme outperforms existing scheme in terms of routing overhead and computational overhead. In [58], the authors proposed a solution to detect black hole attacks, which is similar to [57]. The proposed method also uses fabricated RREQ message and next hop information to mitigate malicious nodes. Results showed that it reduces 70% end-to-end delay, and increases 12% throughput and 45% PDR with compared to standard AODV. However the technical novelty of the paper is thin because the used methods were proposed by other researchers in existing papers. In [59], the authors proposed the placebo packet protocol (PPP) to detect black hole attacks and to identify malicious routers. In PPP, a trusted source node sends a fake data packet as well as the placebo packet, which is similar to [57] and [58]. The difference to them is that the placebo packet is sent along a pre-determined Hamiltonian path and traverses all routers. A malicious node is detected because it

recognizes the placebo packet as a regular data packet and drops the packet. Simulation results showed that the PPP is capable of finding malicious nodes. In addition, the larger network scale needs to use more placebo packets to find malicious nodes. Last, the researchers did not compare the PPP solution with existing schemes in simulations.

In [60], the authors proposed the cluster and reputation based cooperative malicious node detection and removal (CRCMD&R) scheme. In CRCMD&R scheme, the cluster head node ID of originator field records the cluster head's ID after it left the originator. In RREP packet, it records the node ID, the next node of the node sent RREP, prime product number, and the cluster head's ID of the node sent RREP. Three additional tables are needed in CRCMD&R scheme, i.e., neighbor, legitimacy value and reputation level tables. In neighbor table, node ID and cluster head's ID are recorded in each cluster head. In legitimacy value table, it records node ID, success count, total count and legitimacy value. The legitimacy value obtained from the success count divided by total count. In reputation level table, the promiscuous mode [20] is applied to cluster heads to calculate the reputation. The reputation value is calculated as the node sent RREP to the next node of the node sent RREP. The reputation levels are classified into four levels, i.e., malicious, suspect, less trustworthy and trustworthy. Simulation results showed that the CRCMD&R scheme outperforms standard AODV with higher total throughput. However the used methods are old-fashioned that were proposed by other researchers except the new idea of using cluster technique.

5. Other Attacks in MANET

In this section, other attacks in MANET are introduced and studied, e.g., denial-of-service (DoS), wormhole, flooding and routing attacks. The comparison of these attacks in MANET is captured in Table 4. Since a vast number of papers have been proposed, we study parts of representative papers.

With abnormal behavior detection, Tsai [61] proposed an incremental particle swarm optimization (IPSO) algorithm to enhance the performance of IDS. First of all, the IPSO classifies the type of network flows from training data set in the classification phase. Then it classifies the new incoming patterns in the clustering phase. The proposed IPSO algorithm can be applied to classify normal routing patterns and informal routing patterns for detecting black hole attacks in MANET. In [62], the authors investigated how classification performance depends on the cost matrix for intrusion detection in MANET. Five well-known classification algorithms are examined with a number of network metrics. The performance of these algorithms are analyzed under four types of attacks in MANET, i.e., black hole, data forging, packet drop and flooding attacks. In [63], the authors proposed an intrusion detection method based on probabilistic analysis. The k-dimensional feature space of multivariate normal distribution is used to apply anomaly detection on the distribution. Moreover, the Mahalanobis distance of normally distributed data is used to identify normal data and abnormal data.

With wormhole attacks, Jhaveri et al. [64] surveyed DoS attacks in MANET, e.g., blackhole, wormhole, grayhole attacks. They not only introduced the operation of these attacks but also surveyed parts of existing schemes on detection and prevention. In [65], the authors aimed at proposing a secure IDS to prevent distributed DoS (DDoS) attacks in MANET. The main concept of the paper is to use more and different parameters in the IDS, however the used parameters were not clarified clearly. In

[66], the authors proposed an IDS called Enhanced Adaptive ACKnowledgment (EAACK) for MANET. The difference between EAACK with their previous work [67] is that the EAACK scheme uses digital signature to prevent attackers forging acknowledgment signature. In [68], the authors utilized analytical hierarchy process to elect special nodes for preventing wormhole attacks in MANET. A bi-directional wormhole location mechanism is further proposed to tackle with collaborative black hole attack.

Table 4. Comparison of other attacks in MANET

Scheme	*Publication year*	*Attack type*	*Routing protocol*	*Simulator*
IPSO [61]	2013	Abnormal behavior	-	Self-programmed C++
Cost matrix [62]	2013	Flooding, forging, packet dropping and black hole attacks	AODV	GloMoSim
Probabilistic model [63]	2017	Anomaly detection	-	-
Jhaveri et al. [64]	2012	Wormhole, Blackhole and Grayhole attacks	-	-
Secure IDS [65]	2012	Distributed denial-of-service	AODV	NS-2 (v. 2.31)
EAACK [66]	2013	Forging attack	DSR	NS-2 (v. 2.34)
Bi-directional wormhole location [68]	2013	Wormhole attack	AODV	-
Traffic flooding attack detection [69]	2013	TCP-SYN flooding, ICMP flooding and UDP flooding attacks	-	Stacheldraht
DDWS [70]	2014	Flooding attack	AODV	NS-2
Anonymous secure routing protocol in [71]	2013	Routing attack	-	-
Lightweight scheme based on RSS [72]	2013	Sybil attack	-	NS-2 (v. 2.30)

The symbol "-" means unmentioned.
IPSO=Incremental Particle Swarm Optimization, IDS=Intrusion Detection System, EAACK=Enhanced Adaptive ACKnowledgment, DDWS=Dual Defensive Wall System, RSS=Received Signal Strength.

In [69], the authors proposed a traffic flooding detection method and implemented it named the in-depth analysis system. The proposed system based on data mining technique classifies attack types, e.g., TCP-SYN flooding, ICMP flooding and UDP flooding attacks. In [70], the authors proposed an approach for reducing redundant RREQ packets by the cooperation of destination and the neighbor nodes where within one-hop distance from malicious node. In [71], the authors proposed the anonymous secure routing protocol with privacy preservation to establish a secure route. The anonymous secure routing protocol is established based on the proposed neighbor discovery scheme to connect all neighbor nodes with symmetric or asymmetric links. In [72], the authors proposed a lightweight scheme to detect Sybil attacks in MANET based on received signal strength. The proposed scheme detects Sybil identities without using centralized third party or extra hardware.

6. Open Issues and Future Trends

Although security issues in MANETs have been investigated for many years, there are still various open issues of detecting black hole attacks, especially the collaborative black hole attack. We believe that it is not so hard to detect and eliminate a non-cooperative black hole attack (see Section 3) since there are many existing schemes for the problem, but it is still hard to detect and prevent a collaborative black hole attack. Open issues and future trends of black hole detection are discussed as follows.

6.1 Open Issues of Black Hole Detection

Frist of all, how to choose the best detection/prevention method according to used routing protocol is a dilemma problem. No matter what scheme used, it has pros and cons. For example, a detection scheme based on reactive routing protocol reduces routing overhead but suffers from slight packet loss when routing starts. On the contrary, a detection method lies on proactive routing protocol yields higher PDR but leads to more routing overhead due to periodical broadcast. For this reason, when proposing a detection/prevention method for black hole attacks in MANETs, the critical issue is how to promptly detect malicious nodes without raising overhead.

A non-cooperative black hole attack can be easily detected by various methods, e.g., examination of RREQ and RREP packets, trust value of mobile nodes, check of data routing information in one or two-hop neighbors, usage of destination sequence number. However it is still hard to detect and eliminate collaborative black hole attacks correctly. Two black hole nodes are willing to collude in forging false information or fake packets for achieving their misbehavior. The existing schemes for non-cooperative black hole attacks will be failed in detecting collaborative malicious nodes. The detection and prevention of collaborative black hole attacks still need to overcome with great efforts.

Last, system performance is a vital issue to detect and prevent malicious attacks but challenging. No matter what scheme used, it trades certain overhead off for detection accuracy, e.g., more routing overhead for higher PDR, larger end-to-end delay for higher network throughput, higher computation load for higher PDR. For this reason, when applying detection and prevention method, the critical issue is how to trade suitable performance metrics off based on the major object, e.g., the highest PDR or network throughput, or the lowest routing overhead or end-to-end delay.

6.2 Future Trends of Black Hole Detection

There is no doubt at all that collaborative black hole detection method will still be a hot research issue in the future. In our opinion, a hybrid routing protocol is essential to improve the defects of reactive and proactive routing protocols. Except the well-known ZRP and TORA routing protocols, the integration of reactive and proactive routing protocols is also a favorable solution. For instance, it is proper to use an on-demand routing method at the beginning and to apply table-driven routing method when network topology changes. As a result, the packet loss problem of reactive routing and the redundant routing overhead of proactive routing can be improved.

In order to discover collaborative black hole attacks, we had proposed a brand-new detection concept, viz. cooperative bait detection scheme [46,47,52]. First of all, a hybrid routing protocol was proposed by composing reactive and proactive routing methods to improve their defects. In practice,

DSR is adopted in our hybrid routing protocol. The primary idea is that source node sends bait RREQ packets with empty target address before route discovery. Note that the bait RREQ packets only survive a while to economize the use of network throughput. Black hole nodes can be easily found because they reply forged RREP packets with destination address to the source node. As a result, source node is capable of recognizing malicious nodes because it should not receive any reply packet due to the design of empty target address. The brand-new idea can be applied to all routing protocols with a slight modification.

According to this survey, we found that there is a novel tendency to detect black hole nodes. A few of researchers start to utilize metaheuristic or evolution-based algorithms to tackle with black hole attacks, e.g., GA [22], ACO [23] and GA with fuzzy logic [36]. A metaheuristic algorithm has a higher probability of finding malicious nodes and detecting abnormal operations through its evolution and training process. However a comprehensive scheme for black hole detection is still unseen. Furthermore, it needs more time to complete evolution and training process but attack detection should be instantaneous. In other words, an evolutionary algorithm with significant computation complexity may not fit in with the malicious node detection at once. We deem that some modifications of these algorithms are necessary for detecting collaborative black hole attacks in MANETs.

7. Conclusions

A vast number of papers on black hole detection in MANET have been published during past five years. In this survey, we study and discuss various schemes for detecting malicious attacks in MANETs. The black hole attacks are surveyed and classified into non-cooperative and collaborative black hole attacks. More than 25 schemes for non-cooperative black hole attack detection are studied and compared to point out their pros and cons. At least 14 schemes of collaborative black hole attack detection are investigated to show the state-of-the-art research status. In addition, other attacks in MANETs are also investigated such as DoS, wormhole, flooding and Sybil attacks. According to the survey result, we list a number of open issues and provide some future trends for the reader and audience of the paper. We expect to facilitate more scholars and researchers to grasp black hole detection in MANETs.

Acknowledgement

This research was partly funded by the Ministry of Science and Technology (MOST), Taiwan, R.O.C. under grant (No. 105-2221-E-197-010-MY2, No. 106-2511-S-259-001-MY3, and No. 106-2811-S-259-001).

References

[1] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," *in Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, TX, 1998, pp. 85-97.

[2] A. Nadeem and M. P. Howarth, "A Survey of MANET intrusion detection & prevention approaches for network layer attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2027-2045, 2013.

[3] F. H. Tseng, L. D. Chou, and H. C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Human-centric Computing and Information Sciences*, vol. 1, article no. 4, 2011.

[4] E. M. Royer and C. K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Communications*, vol. 6, no. 2, pp. 46-55, 1999.

[5] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, New Orleans, LA, 1999, pp. 90-100.

[6] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, vol. 353, pp. 153-181, 1996.

[7] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proceedings of Conference on Communications Architectures (SIGCOMM '94), Protocols and Applications*, London, UK, 1994, pp. 234-244.

[8] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Proceedings of the IEEE International Multi Topic Conference (INMIC): Technology for the 21st Century*, 2001, pp. 62-68.

[9] V. Park and S. Corson, "Temporally-ordered routing algorithm (TORA) version 1: functional specification," The Internet Engineering Task Force, Fremont, CA, *Internet Draft*, 1997.

[10] Z. J. Haas, M. R. Pearlman, and P. Samar, "The zone routing protocol (ZRP) for ad hoc networks," The Internet Engineering Task Force, Fremont, CA, *Internet Draft*, 2002.

[11] R. Lakhwani, S. Suhane, and A. Motwani, "Agent based AODV protocol to detect and remove black hole attacks," *International Journal of Computer Applications,* vol. 59, no. 8, pp. 35-39, 2012.

[12] N. Sharma and A. Sharma, "The black-hole node attack in MANET," in *Proceedings of 2nd International Conference on Advanced Computing & Communication Technologies*, Rohtak, India, 2012, pp. 546-550.

[13] M. Al-Shurman, S. M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks," in *Proceedings of the 42nd Annual ACM Southeast Regional Conference*, Huntsville, AL, 2004, pp. 96-97.

[14] N. R. Yerneni and A. K. Sarje, "Secure AODV protocol to mitigate black hole attack in mobile ad hoc," in *Proceedings of 3rd International Conference on Computing Communication & Networking Technologies (ICCCNT),* Coimbatore, India, 2012, pp. 1-5.

[15] F. Thachil and K. C. Shet, "A trust based approach for AODV protocol to mitigate black hole attack in MANET," in *Proceedings of International Conference on Computing Sciences*, Phagwara, India, 2012, pp. 281-285.

[16] R. K. Bar, J. K. Mandal, and M. M. Singh, "QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack," *Procedia Technology*, vol. 10, pp. 530-537, 2013.

[17] S. Biswas, T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," in *Proceeding of Applications and Innovations in Mobile Computing (AIMoC)*, Kolkata, India, 2014, pp. 157-164.

[18] A. Sharma, R. Singh, and G. Pandey, "Detection and prevention from black hole attack in AODV protocol for MANET," *International Journal of Computer Applications*, vol. 50, no. 5, pp. 1-4, 2012.

[19] P. K. Singh and G. Sharma, "An efficient prevention of black hole problem in AODV routing protocol in MANET," in *Proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, UK, 2012, pp. 902-906.

[20] K. Vishnu and A. J. Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," *International Journal of Computer Applications*, vol. 1, no. 22, pp. 38-42, 2010.

[21] P. Jaiswal and R. Kumar, "Prevention of black hole attack in MANET," *International Journal of Computer Networks and Wireless Communications*, vol. 2, no. 5, pp. 599-606, 2012.

[22] N. Mistry, D. C. Jinwala, and M. Zaveri, "Improving AODV protocol against blackhole attacks," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, Hong Kong, pp. 1034-1039, 2010.

[23] L. Tamilselvan and V. Sankaranarayanan, "Prevention of blackhole attack in MANET," in *Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)*, Sydney, Australia, 2007, pp. 21-21.

[24] K. S. Sujatha, V. Dharmar, and R. S. Bhuvaneswaran, "Design of genetic algorithm based IDS for MANET," in *Proceedings of International Conference on Recent Trends in Information Technology*, Chennai, India, 2012, pp. 28-33.

[25] R. Kumar and R. Chadha, "Mitigation of black hole attack using generic algorithms and fuzzy logic," *International Journal of Engineering Sciences & Research Technology*, vol. 5, no. 6, pp. 818-826, 2016.

[26] Sonia and H. Kaur, "Proficient and enhance the mobile ad-hoc network using routing protocol and EBFOA (Enhanced Bacteria Foraging Optimization Algorithm)," *International Journal of Modern Computer Science*, vol. 4, no. 6, pp. 88-94, 2016.

[27] K. M. Passino, "Biomimicry of bacterial foraging for distributed optimization and control," *IEEE Control Systems*, vol. 22, no. 3, pp. 52-67, 2002.

[28] K. S. Sowmya, T. Rakesh, and D. P. Hudedagaddi, "Detection and prevention of blackhole attack in MANET using ACO," *International Journal of Computer Science and Network Security*, vol. 12, no. 5, pp. 21-24, 2012.

[29] D. G. Kariya, A. B. Kathole, and S. R. Heda, "Detecting black and gray hole attacks in mobile ad hoc network using an adaptive method," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 1, pp. 37-41, 2012.

[30] I. Woungang, S. K. Dhurandher, M. S. Obaidat, and R. D. Peddi, "A DSR-based routing protocol for mitigating blackhole attacks on mobile ad hoc networks," *Security and Communication Networks*, vol. 9, no. 5, pp. 420-428, 2016.

[31] M. Mohanapriya and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," *Computers and Electrical Engineering*, vol. 40, no. 2, pp. 530-538, 2014.

[32] S. Kumar and K. Dutta, "Intrusion detection technique for black hole attack in mobile ad hoc networks," *International Journal of Information Privacy, Security and Integrity*, vol. 2, no. 2, pp. 81-101, 2015.

[33] M. Patel and S. Sharma, "Detection of malicious attack in MANET a behavioral approach," in *Proceeding of 3rd IEEE International Advance Computing Conference (IACC)*, Ghaziabad, India, 2013, pp. 388-393.

[34] S. Tan and K. Kim, "Secure route discovery for preventing black hole attacks on AODV-based MANETs," in *Proceedings of International Conference on ICT Convergence (ICTC)*, Jeju, Korea, 2013, pp. 1027-1032.

[35] U. Ghosh and R. Datta, "SDRP: secure and dynamic routing protocol for mobile ad-hoc networks," *IET Networks*, vol. 3, no. 3, pp. 235-243, 2014.

[36] T. Varshney, T. Sharma, and P. Sharma, "Implementation of watchdog protocol with AODV in mobile ad hoc network," in *Proceeding of 4th International Conference on Communication Systems and Network Technologies*, Bhopal, India, 2014, pp. 217-221.

[37] S. Shahabi, M. Ghazvini, and M. Bakhtiarian, "A modified algorithm to improve security and performance of AODV protocol against black hole attack," *Wireless Networks*, vol. 22, no. 5, pp. 1505-1511, 2016.

[38] A. Siddiqua, K. Sridevi, and A. A. K. Mohammed, "Preventing black hole attacks in MANETs using secure knowledge algorithm," in *Proceedings of International Conference on Signal Processing and Communication Engineering Systems*, Guntur, India, 2015, pp. 421-425.

[39] A. M. Fahad and R. C. Muniyandi, "Harmony search algorithm to prevent malicious nodes in mobile ad hoc networks (MANETs)," *Information Technology Journal*, vol. 15, no. 3, pp.84-90, 2016.

[40] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao, and C. F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: a cooperative bait detection approach," *IEEE Systems Journal*, vol. 9, no. 1, pp. 65-75, 2015.

[41] M. B. M. Kamel, I. Alameri, and A. N. Onaizah, "STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET," in *Proceedings of IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Chongqing, China, 2017, pp. 1278-1282.

[42] R. Das, B. S. Purkayastha, and P. Das, "Security measures for black hole attack in MANET: an approach," *International Journal of Engineering Science and Technology*, vol. 3, no. 4, pp. 2832-2838, 2011.

[43] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks," in *Proceedings of the International Conference on Wireless Networks*, Las Vegas, NV, 2003, pp. 570-575.

[44] H. Weerasinghe and H. Fu, "Preventing cooperative black hole attacks in mobile ad hoc networks: simulation implementation and evaluation," in *Proceedings of Future Generation Communication and Networking (FGCN 2007)*, Jeju, Korea, 2007, pp. 362-367.

[45] A. A. Bhosle, T. P. Thosar, and S. Mehatre, "Black-hole and wormhole attack in routing protocol AODV in MANET," *International Journal of Computer Science, Engineering and Applications (IJCSEA)*, vol. 2, no. 1, pp. 45-54, 2012.

[46] I. Woungang, S. K. Dhurandher, R. D. Peddi, and I. Traore, "Mitigating collaborative blackhole attacks on DSR-based mobile ad hoc networks," in *Proceedings of the International Symposium on Foundations and Practice of Security*, Montreal, Canada, 2012, pp. 308-323.

[47] J. M. Chang, P. C. Tsou, H. C. Chao, and J. L. Chen, "CBDS: a cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in *Proceedings of 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, Chennai, India, 2011, pp. 1-5.

[48] P. C. Tsou, J. M. Chang, Y. H. Lin, H. C. Chao, and J. L. Chen, "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs," in *Proceedings of 13th International Conference on Advanced Communication Technology (ICACT2011)*, Seoul, Korea, 2011, pp. 755-760.

[49] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 536-550, 2007.

[50] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Personal Communications*, vol. 29, no. 3-4, pp. 367-388, 2004.

[51] G. S. Bindra, A. Kapoor, A. Narang, and A. Agrawal, "Detection and removal of co-operative blackhole and grayhole attacks in MANETs," in *Proceedings of International Conference on System Engineering and Technology (ICSET)*, Bandung, Indonesia, 2012, pp. 1-5.

[52] A. Mishra, R. Jaiswal, and S. Sharma, "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in ad hoc network," in *Proceedings of 3rd IEEE International Advance Computing Conference (IACC)*, Ghaziabad, India, 2013, pp. 499-504.

[53] S. K. Dhurandher, I. Woungang, R. Mathur, and P. Khurana, "GAODV: a modified AODV against single and collaborative black hole attacks in MANETs," in *Proceedings of 27th International Conference on Advanced Information Networking and Applications Workshops*, Barcelona, Spain, 2013, pp. 357-362.

[54] A. A. Aware and K. Bhandari, "Prevention of black hole attack on AODV in MANET using hash function," in *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization*, Noida, India, 2014, pp. 1-6.

[55] R. J. Cai, X. J. Li, and P. H. J. Chong, "A novel self-checking ad hoc routing scheme against active black hole attacks," *Security and Communication Networks*, vol. 9 no. 10, pp. 943-957, 2016.

[56] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in *Proceedings of International Conference on Computer, Communication and Control (IC4)*, Indore, India, 2015, pp. 1-5.

[57] K. S. Arathy and C. N. Sminesh, "A novel approach for detection of single and collaborative black hole attacks in MANET," *Procedia Technology*, vol. 25, pp. 264-271, 2016.

[58] M. Sathish, K. Arumugam K, S. N. Pari, and V. S. Harikrishnan, "Detection of single and collaborative black hole attack in MANET," in *Proceedings of International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2016, pp. 2040-2044.

[59] B. Cerda, E. Martinez-Belmares, and S. Yuan, "Protection from black hole attacks in communication networks," in *Proceedings of the International Conference on Security and Management*, Las Vegas, NV, 2017, pp. 7-11.

[60] S. Sharma and S. Gambhir, "CRCMD&R: cluster and reputation based cooperative malicious node detection & removal scheme in MANETs," in *Proceedings of 11th International Conference on Intelligent Systems and Control (ISCO)*, Coimbatore, India, 2017, pp. 336-340.

[61] C. W. Tsai, "Incremental particle swarm optimisation for intrusion detection," *IET Networks*, vol. 2, no. 3, pp. 124-130, 2013.

[62] A. Mitrokotsa and C. Dimitrakakis, "Intrusion detection in MANET using classification algorithms: the effects of cost and model selection," *Ad Hoc Networks*, vol. 11, no. 1, pp. 226-237, 2013.

[63] J. S. Park, D. H. Choi, Y. B. Jeon, Y. Nam, M. Hong, and D. S. Park, "Network anomaly detection based on probabilistic analysis," *Soft Computing*, 2017. https://doi.org/10.1007/s00500-017-2679-3

[64] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: a survey," in *Proceedings of 2nd International Conference on Advanced Computing & Communication Technologies*, Rohtak, India, 2012, pp. 535-541.

[65] P. Sharma, N. Sharma, and R. Singh, "A secure intrusion detection system against DDOS attack in wireless mobile ad-hoc network," *International Journal of Computer Applications*, vol. 41, no. 21, pp. 16-21, 2012.

[66] E. M. Shakshuki, N. Kang, and T. R. Sheltami, "EAACK–a secure intrusion-detection system for MANETs," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1089-1098, 2013.

[67] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in *Proceedings of the 12th International Conference on Information Integration and Web-Based Applications & Services*, Paris, France, 2010, pp. 216-222.

[68] F. Shi, W. Liu, D. Jin, and J. Song, "A countermeasure against wormhole attacks in MANETs using analytical hierarchy process methodology," *Electronic Commerce Research*, vol. 13, no. 3, pp. 329-345, 2013.

[69] J. Yu, H. Kang, D. H. Park, H. C. Bang, and D. W. Kang, "An in-depth analysis on traffic flooding attacks detection and system using data mining techniques," *Journal of Systems Architecture*, vol. 59, no. 10, pp. 1005-1012, 2013.

[70] F. C. Jiang, C. H. Lin, and H. W. Wu, "Lifetime elongation of ad hoc networks under flooding attack using power-saving technique," *Ad Hoc Networks*, vol. 21, pp. 84-96, 2014.

[71] R. J. Hwang and Y. K. Hsiao, "An anonymous distributed routing protocol in mobile ad-hoc networks," *The Journal of Supercomputing*, vol. 66, no. 2, pp. 888-906, 2013.

[72] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight Sybil attack detection in MANETs," *IEEE Systems Journal*, vol. 7, no. 2, pp. 236-248, 2013.

Fan-Hsun Tseng https://orcid.org/0000-0003-2461-8377

He received his Ph.D. degree in Computer Science and Information Engineering from National Central University, Taoyuan, Taiwan, in 2016. He is currently an assistant professor with the Department of Technology Application and Human Resource Development, National Taiwan Normal University, Taipei, Taiwan. Dr. Tseng has been the Associate Editor-in-Chief for Journal of Computers since May 2016. His research interests include cloud computing, IoT applications, 5G mobile networks.

Hua-Pei Chiang

She received her Ph.D. degree in Engineering Science from National Cheng Kung University, Tainan, Taiwan in 2016. She is currently a senior director with the Network and Technology Division, FarEasTone Telecommunications Co. Ltd., Taipei, Taiwan. Her research interests include network management, network security, 4G, 5G, wireless sensor network and cloud computing.

Han-Chieh Chao https://orcid.org/0000-0003-3222-1708

He received his M.S. and Ph.D. degrees in Electrical Engineering from Purdue University, West Lafayette, Indiana, in 1989 and 1993, respectively. He is currently a professor with the Department of Electrical Engineering, National Dong Hwa University, where he also serves as president. He is also with the Department of Computer Science and Information Engineering and the Department of Electronic Engineering, National Ilan University, Taiwan; College of Mathematics and Computer Science, Wuhan Polytechnic University, Wuhan, China, and Fujian University of Technology, Fuzhou, China. He serves as the Editor-in-Chief for the Institution of Engineering and Technology Networks, the Journal of Internet Technology, the International Journal of Internet Protocol Technology, and the International Journal of Ad Hoc and Ubiquitous Computing. He is a Fellow of IET (IEE) and a Chartered Fellow of the British Computer Society.