Comprehensive Review of Collaborative Network Attacks in MANET

Oluwafemi Tolulope Fasunlade (*Corresponding author*) and **Shikun Zhou**

School of Computing

David Sanders

School of Mechanical & Design Engineering

University of Portsmouth

***Abstract*— This paper considers multiple network attacks in a Mobile Ad hoc Network (MANET). MANET is a type of network that does not require any infrastructure for nodes to communicate with each other. The general assumption in MANET is that each node is a trusted node. However, due to its lack of infrastructure and dynamic topology, the MANET is exposed to network layer attacks. In this paper, some of the network layer attacks such as the black hole attack, worm hole attack and gray hole attack are discussed. Frequent multiple network attacks are highlighted, and the identification of collaborative network attacks is discussed. There are several symptoms and observations in a network that signal the presence of an attack and some of the symptoms of these attacks will be highlighted. Finally, an analysis of existing multiple network attacks will be discussed, and the identification of prospective multiple network attacks is considered.**

Keywords*— *MANET, AODV, blackhole, wormhole, gray hole

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a self-organized and self-configuring temporary network of independent mobile nodes connected by wireless links. There is no fixed infrastructure or centralized administration in this type of network [1]. With the widespread availability of cheaper, smaller and more powerful mobile devices, MANETs have grown into one of the fastest areas of research. MANETs have been widely used in several applications such as emergency operations, disaster relief, military crisis operations, maritime communications, vehicle networks, business meetings, and site networks [2].

In ad hoc networks, mobile nodes can move, join and leave the network dynamically and routes need to be updated frequently due to its dynamic nature. The nodes in MANETs communicate with one another via wireless links and act both as a host and a router. Packets are forwarded to the correct node in a network after route establishment to transfer their information to other nodes [3]. For instance, a network consisting of mobile nodes where node (X) is a source node and node (Y) is a destination node as shown in figure 1. Node (X) can communicate with node (Y) by using the shortest path {X-A-D-Y} but if node (A) moves out of range with node (X), then node (X) has to seek an alternative route to node (Y) possibly using the path {X-B-C-D-Y}.

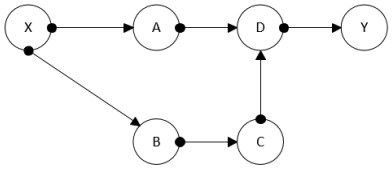

Fig. 1. Communication between nodes in MANET

A variety of new protocols have been developed for finding and updating routes as well as providing communication between nodes. It should be noted that no proposed routing protocol has been accepted as standard yet and existing routing protocols suffer from new forms of attacks [1]. Much research has been done to detect and prevent attacks against existing routing protocols in MANET. That research includes secure routing protocols and intrusion detection systems.

MANETs are more vulnerable to malicious attacks than wired networks due to their open mediums and continuously changing network topologies. Thus, malicious attackers are able to learn ways of changing the information of a particular data packet. In such cases, it is important to have an efficient intrusion detection system (IDS) in place to protect MANETs from attacks and enhance their security levels [4].

Much existing research work concerning MANETs dealt with prevention and detection approaches to combat individual node attack. In this regard, the effectiveness of these approaches can become weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result in more devastating damage to the network. It is possible for a MANET to be vulnerable to different types of attacks simultaneously [5]. This paper presents a fundamental understanding of one of the existing routing protocols, Ad hoc On Demand Vector (AODV) routing protocol. Furthermore, an overview of the network attacks that affect MANET will be investigated, finishing with multiple and collaborative attacks and how they might be detected.

II. AD HOC ON-DEMAND DISTANCE VECTOR

AODV routing protocol plays a role in identifying and transmitting packets from a source node to a destination node through intermediate nodes. AODV requests a route when it needs to send a packet from a source node to its destination node [4] as seen in Fig 2. AODV includes three messages: route request (RREQ), route reply (RREP) and route error [6]. In AODV, each node has its own sequence number, this number increases a change in links; where a high sequence indicates the latest route. For example, when a source node wishes to route a packet to a destination node, the source node initiates route discovery, a source node broadcasts an RREQ message with the sequence number. Each of the intermediate nodes checks if it has fresh route to the destination node [6]. The respective intermediate nodes compare the sequence numbers with the sequence number in the RREQ packet. If the sequence number of the receiving node is greater than the sequence number in the RREQ message, it will generate a unicast RREP message to the source node. However, if the sequence number of the receiving node is less than the sequence number in the RREQ message, it will further broadcast the RREQ to other nodes. Eventually, the source nodes will get RREP packets from multiple nodes and accept the path with a higher sequence number, because a high sequence number is seen as an updated path [7]. Every mobile node maintains a routing table that consists of route

directions to the destination. The AODV keeps information about routing tables but only recent routes. If an entry is not used, it eventually discards it [8].

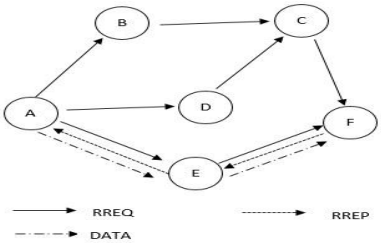

Fig. 2. AODV Protocol

III. Network Attacks On Manet

MANETs are vulnerable to Denial of Service (DoS) attacks on the network layer. These attacks can be classified into three types: Routing disruption, Forwarding disruption and Resource consumption attacks [4]. Routing disruption is caused by wormhole attack, black hole attack and gray hole attack. Also, Jellyfish, directional antenna abusing are forward disruption attacks, while control packets flood and packet injection attacks are resource consumption attacks [9]. However, the focus of this paper is on routing disruption attacks.

A. Blackhole Attack

In Black hole attacks, a malicious node exploits the vulnerabilities of the route discovery procedure of AODV by advertising the wrong paths as good paths to the source node. The malicious node sends a RREP with a destination sequence number larger than the sequence number in the RREQ message, thus indicating that it has a fresh route to the destination [10]. The source node then selects this route and the malicious node captures all data forwarded on that route and creates a hole in the network. The malicious node completely discards the traffic [7]. In the presence of a black hole attack, no traffic along that route is delivered. In Fig 3, node C acts as the black hole node. Hence, all traffic from source node A to destination node F is dropped. The performance of the network is degraded as a result of this attack.

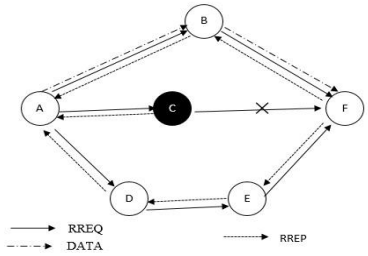

Fig. 3. Blackhole attack

B. Wormhole Attack

In wormhole attacks, a malicious node captures data at one point in a network and sends them through a tunnel to another malicious node as seen in Fig 4. The tunnel creates an illusion to the source node that the two malicious nodes are one hop away and hence provides the shortest path to the destination. The creation of the tunnel increases their chances of being selected as part of the route and they then attempt to drop all incoming and outgoing packets, causing a denial of service in the network [8]. A tunnel can be established by either an In-Band Channel or Out-Band Channel. In an Out-Band Channel the colluding malicious nodes establish a direct link between the two colluding nodes by long range wireless transmission or by a private high-speed network. On the other hand, In an In-band channel it uses encapsulation to develop a covert overlay tunnel over the existing wireless medium. Wormhole attack is possible even if all communications provide authenticity and confidentiality[11]. The wormhole attack can be launched individually or collaboratively. In wormhole attacks, the return trip time (RTT) of packets appear shorter and rate of packet delivery is faster than usual. Not every wormhole is malicious, therefore in the presence of malicious activity, packets can be dropped between the two wormhole nodes, thereby degrading the performance of the network [12].

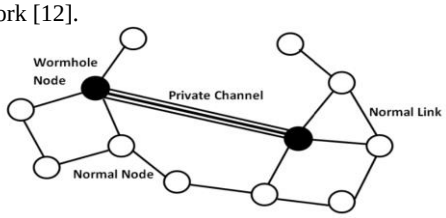

Fig. 4. Worm Hole attack

C. Gray Hole Attack

Gray hole attacks (sometimes referred to as selective forwarding) consist of two phases. In the first phase the malicious node exploits the vulnerabilities of the route discovery process of the routing protocol by advertising itself as having a valid route to destination while in the second phase, the malicious node drops the intercepted packets with a certain probability. For instance, the attacker may drop packets coming from specific nodes while forwarding all the packets for other nodes or it may drop packets for some time and behave normally for the rest of the time. Gray hole attack detection is difficult [10]. In a gray hole attack, the malicious node can simply drop packets coming to it from some specific nodes, while it forwards the others. Also, gray hole could happen for particular time duration, where packets are transmitted at a particular period of time and dropped for a certain duration. Finally, gray hole attack could drop packets randomly while forwarding the remaining packets. Gray hole attack is a variation of black hole attack and is more difficult to detect [5].

IV. Collaborative Network Attacks

There have been several attempts to detect multiple attacks working individually or collaboratively in MANET and other network types. This section considers combined attacks under any network type.

A. Blackhole and Gray hole attacks

Woungang [5]proposed a cooperative bait detection system (CBDS) approach to detect collaborative black hole or gray hole attacks. This approach was implemented using AODV routing protocol in order to reduce routing overhead associated with CBDS using Dynamic Source Routing (DSR) protocol. The results show that CBDS using DSR performs better than the standard DSR protocol. Likewise, simulation results show that CBDS using AODV performs better than CBDS using DSR in terms of throughput and packet delivery ratio.

An improved bait detection system (IBDS) approach over AODV routing protocol was proposed to detect network attacks [13]. The IBDS combines proactive and reactive schemes to save resources. The results show reductions in energy consumption and routing overhead as well as an increase in packet delivery ratio. This approach could also be used to detect other attacks such as wormhole attack and denial of service.

Rana [14] proposed an enhanced, modified AODV for detecting and preventing malicious nodes in MANETs in the presence of single individual attacks or collaborative black hole and gray hole attacks. The simulation results show that this method performs better than the standard AODV routing protocol in detecting individual and collaborative attacks. The network metrics used were routing overhead, packet delivery ratio and throughput. The proposed approach was not efficient in a large network as its routing overhead increased with increase in network size. The attack cooperation was between nodes of black hole attack.

Singh Bindra et al [15] proposed a modified AODV routing protocol using a data routing information (DRI). The DRI is used at

each node and a cross-checking method was performed to detect cooperative black hole nodes and gray hole attacks in the network. The protocol could also discover secure paths from the source to the destination node. This method could only work when the malicious nodes were consecutive while operating in cooperation. Thus, non-consecutive cooperating nodes could not be detected.

In [16] an approach was proposed to defend against a black hole attack and selective forwarding attack in a wireless sensor network. The proposed technique used an updated active trust scheme and data routing scheme along with data type checking during routing. The Elliptic-Curve Cryptography (ECC) algorithm was also used to enhance the privacy of data by encrypting it before the routing started. The method could only defend against these attacks individually and not when in collaboration with each other.

In [10], a method was proposed to detect and prevent black, gray and cooperative black hole attacks in MANET over AODV routing protocols. The technique used a multi-level mobile backbone network. The technique also involved the trust value of mobile nodes as well as their location and power. The proposed technique performed better than standard AODV, intrusion detection system techniques and hash-function techniques. Furthermore, the technique could only tackle cooperation between similar attacks and not different attacks.

B. Blackhole and Wormhole attacks

In [17], a trusted secure AODV routing protocol was proposed to alleviate the effects of unified attacks such as black hole, worm hole and collaborative black hole attacks in MANET. The attacks were simulated simultaneously on a network. The results obtained showed better performances using network metrics like packet delivery ratio, end to end delay and throughput as compared to standard AODV protocol.

Mehta [18] demonstrated the performances of MANETs using network parameters such as throughput and packet delay against black hole attack and wormhole attack. However, the focus of the paper was on the individual impacts of these attacks. The routing protocol AODV was implemented, and the results show how data loss confirmed the presence of these attacks as well as the impact on network connectivity. Kaur [7] proposed a technique to defend black hole and wormhole attack in a wireless sensor network as well as helping to increase network lifetime. This is different from the traditional way of proposing one single approach to mainly defending from one type of attack. However, the author did not provide any simulation or results to support the proposed algorithms.

Patidar [19] proposed a protocol based on the concept of a specification-based detection system to detect black hole attack and a hop count analysis approach to detect wormhole attack in a MANET. The results show that increasing the number of nodes does not affect the performance of these strategies. Rather it is the mobility of the nodes that affect the routing protocols most. The proposed protocols showed superior performance as throughput and packet delivery ratio increases. However, these protocols led to an increase in the average end to end delay

C. Wormhole and Gray hole attacks

In [20], a lightweight trust mechanism for securing Routing Protocol for Low Power Lossy network (RPL) against wormhole and gray hole attacks was proposed. The proposed method used direct trust which was computed based on node properties and Indirect Trust which is based on opinion of the neighbouring nodes. However, it could not detect collaborative wormhole and gray hole attacks**.**

V. TACKLING COLLABORATIVE ATTACKS

Collaborative network attacks are not limited to MANET but can exist in other network systems [21] and cyber physical systems [22][23]. The way to tackle collaborative network attacks is by detecting the anomalies that could be present in the network. So, to detect collaborative network attacks, some symptoms have to be known. These symptoms include the status of the route request queries (RREQ), route request replies (RREP) and the transmitted data. At the moment, only symptoms and observations of individual network attacks have been highlighted. However new symptoms and observations are required to efficiently identify and tackle collaborative network attacks.

Symptoms of network attacks are collections of network anomalies caused by malicious nodes. Each symptom can be separated into a set of activities of an attacker. The activities of a malicious node can be observed. The observations are a list of misuse of packets exchanged in a network. The observations consist of data packets misuse, and incorrect routing packets in a MANET [24].

Some of the observations in these attacks include modified RREQ and RREP packets, delay and loss of RREQ, RREP and data packets. However, an uncommon observation of the blackhole and gray hole attack is a surge of RREQ and RREP packets. While in wormhole attack, the unusual observation is the encapsulation of RREQ, RREP and Data packets [25]. One or more observations can determine symptoms listed in Table 1.

Table 1. Symptoms of Network attacks

Symptoms/Attack type	Blackhole	Wormhole	Gray hole
Low hop count route replies	YES	YES	YES
Increased packet delivery time	NO	YES	NO
Number of neighbours increased	YES	YES	YES
Large propagation delays	NO	YES	NO
Reception of same message	NO	YES	NO
More load on certain nodes	NO	YES	NO
RREQ is not broadcast by malicious nodes	YES	YES	YES
Data stops transmitting from certain nodes	YES	NO	NO
Quick RREP	YES	NO	YES
Similar hop count to various destinations	YES	NO	YES
Congestion in Network	YES	NO	YES
Data packet loss	YES	NO	YES
Presence of asymmetrical links	NO	YES	NO

Increase in the number of neighbours, low hop count replies and non-broadcast of RREQ by malicious nodes are symptoms that can indicate the behaviour of black hole, wormhole and gray hole attacks. These symptoms are influenced by encapsulation of packets, rushing of RREQ and RREP packets and modification and sending of fake RREP.

Increase in packet delivery time, reception of the same message and presence of asymmetrical links indicate the presence of a wormhole attack. These symptoms are primarily due to the creation of a tunnel between the wormhole nodes.

Similar hop counts to various destinations, the sending of quick RREP, and occurrence of data loss indicate the behaviour of black hole and gray hole attacks. However, in a black hole attack, the malicious node stops sending packets entirely while in a gray hole attack, randomly selected packets are sent.

The occurrence of considerable propagation delay and fluctuating data losses in the network alludes to the presence of wormhole and gray hole attacks. These symptoms are the basis on which proposed detection method is evaluated.

Table 1 lists individual symptoms for network attacks. However, a collaborative attack such as a wormhole and gray hole attack could involve a combinations of some of these symptoms.

Two common symptoms to indicate a possible collaborated wormhole and gray hole attack, are *large propagation delay* and *unusually high or fluctuation of data packet*. Initial experiments confirm these newly discovered symptoms. Some simultaneous procedures have been carried out which don't require any special hardware. Furthermore, the initial method addressed in early experiments utilised a blacklist and a local clock.

The concept of RTT and packet forwarding ratio is used to notice the occurrence of these attacks. If a source node requires a route to a destination node, it initiates a route discovery and sends the packet through a designated route. The source node collects the round trip time (RTT) of each intermediate node the packets goes through and computes the RTT values of two successive nodes. These RTT values should be the same or similar. A wormhole attack will result in an unusual pattern of such pairs of RTT values. Possible collaborated attacks will cause significant increases between the pairs of RTTs. Initial experiments have shown these symptoms, however further investigations and developments will be needed. These experiments are analysed elsewhere.

In addition, every node in the network is set as a monitoring node. Every such node estimates the packet forwarding ratio (PFR) of its neighbouring nodes. If PFR of any node exceeds the threshold, the monitoring node sends an alarm to the source node. The source node adds these malicious nodes to the blacklist and informs other nodes to remove them from their respective routing table and neighbour nodes.

VI. Conclusion

MANETs are vulnerable to network routing disruption attacks such as blackhole, wormhole and gray hole attacks. These attacks could happen individually or in a collaborative manner. In the initial study of this work, it is concluded that the two most likely combinations of collaborative attacks are between blackhole and gray hole attacks, and black hole and wormhole attacks. An initial investigation confirmed that there is no research in the literature to tackle collaborative wormhole and gray hole attacks in MANET. Symptoms associated with network routing attacks were discussed, leading to possible symptoms of collaborative attacks. Furthermore, initial ideas for detecting collaborative wormhole and gray hole attacks have been proposed, investigated and experimented. The proposed method considered RTT and PFR. This method does not require synchronized clocks or any specialised hardware. In future, Investigations will consider more unique symptoms related to collaborative network attacks; particularly the combined wormhole and gray hole attack. The proposed work may be extended using further performance metrics such as packet delivery ratio, routing overhead and end to end delay.

References

[1] S. Kumar, M. Goyal, D. Goyal, and R. C. Poonia, "Routing protocols and security issues in MANET," *2017 Int. Conf. Infocom Technol. Unmanned Syst. Trends Futur. Dir. ICTUS 2017*, vol. 2018-Janua, pp. 818–824, 2018.

[2] S. V. Kumari and B. Paramasivan, "Ant based Defense Mechanism for Selective Forwarding Attack in MANET," *Proc. - Int. Conf. Data Eng.*, vol. 2015-June, pp. 92–97, 2015.

[3] G. Garg, S. Kaushal, and A. Sharma, "Comprehensive study on MANETs network layer attacks," *2013 4th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2013*, 2013.

[4] R. K. Kapur and S. K. Khatri, "Analysis of attacks on routing protocols in MANETs," *Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015*, vol. 5, no. 6, pp. 791–798, 2015.

[5] I. Woungang, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," *IEEE Syst. J.*, vol. 9, no. 1, pp. 65–75, 2015.

[6] 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," *IEEE Int. Conf. Comput. Commun. Control. IC4 2015*, pp. 1–5, 2016.

[7] T. Kaur, "Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol," *2018 IEEE Int. Conf. Smart Energy Grid Eng.*, pp. 288–292, 2018.

[8] P. Khandare and Y. Sharma, "Countermeasures for Selective Forwarding and Wormhole Attack in WSN," in *International Conference on Inventive Systems and Control*, 2017, pp. 1–7.

[9] N. Purohit, R. Sinha, and K. Maurya, "Simulation study of black hole and jellyfish attack on MANET using NS3," *2011 Nirma Univ. Int. Conf. Eng. Curr. Trends Technol. NUiCONE 2011 - Conf. Proc.*, pp. 8–10, 2011.

[10] H. M. Ibrahim, N. M. Omar, and E. K. William, "Detection and Removal of Gray, Black and Cooperative Black Hole Attacks in AODV Technique," *Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 5, pp. 60–70, 2015.

[11] L. Prashar and R. K. Kapur, "Performance analysis of routing protocols under different types of attacks in MANETs," *2016 5th Int. Conf. Reliab. Infocom Technol. Optim. ICRITO 2016 Trends Futur. Dir.*, pp. 405–408, 2016.

[12] F. A. Khan, M. Imran, H. Abbas, and M. H. Durad, "A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks," *Futur. Gener. Comput. Syst.*, vol. 68, pp. 416–427, 2017.

[13] P. L. Chelani and S. T. Bagde, "Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme," *Proc. Int. Conf. Commun. Electron. Syst. ICCES 2016*, pp. 1–6, 2016.

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

[15] G. Singh Bindra, A. Kapoor, A. Narang, and A. Agrawal, "Detection and removal of co-operative blackhole and grayhole attacks in MANETs," *Proc. 2012 Int. Conf. Syst. Eng. Technol. ICSET 2012*, pp. 1–5, 2012.

[16] M. Shinde and D. C. Mehetre, "Black Hole and Selective Forwarding Attack Detection and Prevention in WSN," *2017 Int. Conf. Comput. Commun. Control Autom.*, pp. 1–6, 2017.

[17] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," *2016 Symp. Colossal Data Anal. Networking, CDAN 2016*, pp. 1–6, 2016.

[18] S. Mehta and M. Sharma, "Analysis of Black Hole and Wormhole Attack using AODV Protocol," *Int. J. Res. Manag. Sci. Technol.*, vol. 1, no. 1, pp. 44–48, 2013.

[19] K. Patidar and V. Dubey, "Modification in routing mechanism of AODV for defending blackhole and wormhole attacks," *Proc. 2014 Conf. IT Business, Ind. Gov. An Int. Conf. by CSI Big Data, CSIBIG 2014*, 2014.

[20] R. Mehta, "Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole & Grayhole Attacks," *2018 3rd Int. Conf. Converg. Technol.*, pp. 1–6, 2018.

[21] D. L. Ndzi *et al.*, "Wireless sensor network coverage measurement and planning in mixed crop farming," *Comput. Electron. Agric.*, vol. 105, pp. 83–94, 2014.

[22] D. A. Sanders, D. C. Robinson, M. Hassan, M. Haddad, A. Gegov, and N. Ahmed, "Making decisions about saving energy in compressed air systems using ambient intelligence and artificial intelligence," *Adv. Intell. Syst. Comput.*, vol. 869, no. September, pp. 1229–1236, 2018.

[23] R. Shbib, S. Zhou, and K. Alkadhimi, "SCADA system security, complexity, and security proof," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7719 LNCS, pp. 405–410, 2013.

[24] D. S. K. Tiruvakadu and V. Pallapa, "Confirmation of wormhole attack in MANETs using honeypot," *Comput. Secur.*, vol. 76, pp. 32–49, 2018.

[25] D. S. K. Tiruvakadu and V. Pallapa, "Honeypot Based Black-Hole Attack Confirmation in a MANET: Black-Hole Attack Confirmation," *Int. J. Wirel. Inf. Networks*, vol. 25, no. 4, pp. 434–448, 2018.