A Review of Black Hole Attack on AODV Routing in MANET

Ochola EO
School of Computing
University of South Africa
Pretoria, South Africa
Ocholeo@unisa.ac.za

Eloff MM
School of Computing
University of South Africa
Pretoria, South Africa
Eloffmm@unisa.ac.za

Abstract— **Mobile ad hoc network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized access point such as a base station. MANET has potential applications in very unpredictable and dynamic environments. The nodes, which act as a host as well as a router, communicate to each other through multi hops due to limited transmission ranges. MANETs pose new kinds of security problems, caused by their nature of collaborative, open systems and by limited availability of resources. Unlike other types of network, MANETs are usually deployed without a centralized control unit. Hence, mutual cooperation amongst the participating entities forms the basis for determining the routes to the destination. This aspect makes MANETs vulnerable to various communication security related attacks including *Black Hole* attack. Therefore, the direct application of the conventional routing algorithms is infeasible. *Black Hole* attacks are launched by participating malicious nodes that agree to forward data packets to destination but eavesdrop or drop the packets intentionally, which not only compromise the network, but also degrade network performance. Routing protocols, which act as the binding force in these networks, are a common target of these nodes. According to our analysis, none of the existing attempts to secure MANETs is complete by itself. In this paper, a survey on secure Ad-hoc On-Demand Distance Vector (AODV) routing in MANET against *Black Hole* attack is presented. AODV is a prominent on-demand reactive routing protocol for MANETs based on distance vector routing. The route updates are shared not on a periodic but on an as requirement basis. The control packets create a potential vulnerability that is frequently exploited by malicious nodes. The paper further analyses the impact of *Black Hole* attack in AODV performance.**

Keywords- Mobile ad hoc network (MANET); Secure AODV Routing; Black Hole attack

I. INTRODUCTION

An ad hoc network [1] is a wireless network without any fixed infrastructure. Mobile Ad Hoc Network (MANET) [2] is a group of mobile hosts without the required involvement of any offered infrastructure or centralized access point such as a base station. The MANET presents many challenges, including secure routing, to the research community. Wireless networks are formed by routers and hosts, and use radio frequencies to transmit and receive data instead of using physical cables. Basic networking devices, such as routers or access points are lacking in a MANET. Thus, data transfer among the network nodes is realized by means of multiple hops, and every node acts as a router to establish and maintain routes rather than just serving as a single mobile terminal host [3].

Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. The functioning of ad hoc networks is dependent on the trust and co-operation between nodes. Thus, nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network [4]. A source node intending to transfer data to a destination node located beyond its transmission range do so through intermediate nodes. It is therefore an important issue in MANET to perform a quick route establishment from a source to destination node, a necessity capitalized on by *Black Hole* attack [5].

Based on the routing information update mechanism, the MANET routing protocols can be categorized into proactive (table-driven) protocols, reactive (on-demand) protocols, and Hybrid routing protocols. Proactive routing protocols require that every node proactively searches for routes to other nodes, and periodically exchanges routing messages, in order to ensure that the information in the routing table is up-to-date and correct. Proactive routing protocols include Destination Sequence Distance Vector (DSDV) [6] and Optimized Link State Routing (OLSR) [7]. MANET nodes experience power and bandwidth limitations, thus, continuous transmission of routing messages would lead to network congestion and rapid nodes' power depletion. Reactive routing protocols are also referred to as on-demand routing protocols, as a route is established only when two nodes intend to transfer data. The reactive routing protocols include Ad hoc On-Demand Distance Vector (AODV) [8] and Dynamic Source Routing (DSR) [9]. A route request (RREQ) message is generally broadcasted to the entire network through flooding by a source node during route establishment to the destination node. Hybrid protocols utilize both proactive and reactive approaches. They offer possibilities to dynamically switch between the proactive and reactive parts of the protocol.

Security is a major concern in all forms of communication networks. However, ad hoc networks are faced with greater challenges due to their inherent nature, which can be attributed to their characteristics such as: dynamic topology, lack of centralized control, limited battery power and limited bandwidth [10, 11]. Hence, there exist attacks that can be

launched on an ad hoc network. These attacks can be classified based on their nature as either passive or active [12]. Passive attacks illegitimately acquire information by listening to the traffic without disrupting the operation of the routing protocol. However, active attacks alter the flow of data, either by inserting false packets or modifying the packets' contents. Active attacks can further be classified into *external* and *internal* attacks. External attacks are caused by nodes that do not belong to the same network as the victim, whereas internal attacks are caused by nodes that belong to the same network as the victim. That is, these attacks are carried out by an internal compromised node or external advisory.

The MANET routing protocols are vulnerable to routing attacks [13]. The *active* routing attacks in MANET can be classified into five broad categories: attacks using impersonation, modification, fabrication, replay, and Denial of Service (DoS). The most popular routing protocol, which has been extensively discussed in research papers, is AODV [8]; therefore, this study focuses on *Black Hole* attack detection and prevention scheme on an AODV-based MANETs. AODV minimises the number of required broadcasts by creating routes on a demand basis, as it is a pure on-demand route acquisition system. Nodes that are not on a selected path neither maintain routing information nor participate in routing table exchanges [14].

II. Security Issues

Security [15] is much more difficult to maintain in MANETs due to their vulnerability, than wired networks. The use of wireless links render an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and distortion [16, 17, 18]. The MANET vulnerabilities include, but not limited to the following [19, 20]:

a) Dynamically changing network topology: mobile nodes join and leave the network arbitrarily, resulting to dynamic change of network topology. This allows a malicious node to join the network without prior detection.
b) Lack of centralized monitoring: there is absence of any centralized infrastructure that prohibits any monitoring mechanism in the network. This makes the classical security solutions based on certification authorities and on-line servers inapplicable. Even the trust relationships among individual nodes also changes, especially when some nodes are found to be compromised. Hence, security mechanisms need to be on the dynamic and not static.
c) Cooperative algorithms: MANET routing algorithms require mutual trust between neighbouring nodes, which violates the principles of network security.
d) The absence of a certification authority.
e) The limited physical protection of each of the nodes: network nodes usually do not reside in physically protected places, such as locked rooms. Hence, they can more easily be captured and fall under the control of an attacker.
f) The intermittent nature of connectivity.
g) The vulnerability of the links (open media): messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to the network components. Eavesdropping might give an attacker access to secret information thus violating confidentiality

The security goals for ad hoc networks include confidentiality, availability, integrity, non-impersonation, authentication, non-repudiation and non-fabrication. Whereas, the attacks [21] include *Black Hole* [22], location disclosure [23], replay, blackmail [24], wormhole [18], denial of service [25], routing table poisoning [25], masquerading, passive listening and traffic analysis, breaking the neighbour relationship, and rushing attack [26].

An ad hoc network security attacks can also be broadly categorized as *behavior based attacks* and *location based attacks* [27]. The behavior based attacks can further be classified into passive attacks and active attacks. Passive attacks include eavesdropping of packets containing secrete information, thereby violating the confidentiality principle. It illegally obtains network data packets information without disrupting the communication operation. Whereas, active attacks include delivering data packets to invalid destinations, deleting/dropping packets, modifying packets' contents, and nodes' impersonation; thus violating availability, integrity, authentication and non-repudiation. Active attacks can further be classified as either internal or external.

The contemporary routing protocols for ad hoc networks cope well with the dynamically changing topology but are not designed to accommodate defense against malicious attackers. No single standard protocols capture common security threats and provide guidelines to secure routing [21]. Nodes exchange network topology information in order to establish routes amongst them, which is a potential target for malicious attackers. It is difficult to detect compromised nodes through routing information due to the dynamic topology of ad hoc networks [28]. The routing protocol should be able to bypass the compromised nodes, as long as there are sufficient numbers of valid nodes. However, this needs the existence of multiple, possibly disjoint routes between nodes.

III. AODV Overview

AODV [8, 14, 29] is perhaps the most well-known reactive routing protocol for a MANET [30]. It provides a rapid, dynamic network connection, with low processing loads and low memory consumption. Nodes in the network exchange routing information only when they intend to communicate, and keep this information updated only as long as the communication lasts.

A node intending to send a packet to another node starts a route discovery process in order to establish a route to the destination node, by sending a route request message (RREQ) to its neighbours. Neighbouring nodes increment the hop count on receiving the RREQ, and similarly forward (broadcast) the message to their neighbours using a flooding approach. This continues until the destination node is found. The RREQ

message forwarding has the side effect of making other nodes learn the *reverse route* to the source node. The RREQ message will eventually reach the destination node, which will react with a route reply message (RREP). The RREP is sent as a unicast to the source node along the *reverse route* established during the RREQ broadcast. Similarly, the RREP message allows intermediate nodes to learn a *forward route* to the destination node. Therefore, at the end of the route discovery process, packets can be delivered from the source node to the destination node and vice versa. A route error message (RERR) allows nodes to notify errors due to link breakage, such as when a previous neighbour moves to a new position and is no longer reachable. Each mobile node would periodically send Hello messages (HELLO), thus, each node knows which nodes are its neighbouring nodes within one-hop. Routing messages are either path discovery (RREQ and RREP) or path maintenance (RERR and HELLO) messages. All routing information expires after a timeout in case of an inactive route, and is removed from the routing table.

AODV is a collaborative protocol, allowing nodes to share information about each other. RREQ messages do not necessarily need to reach the destination node during the route discovery process. That is, an intermediate node having a route to the destination simply generates the RREP without any further forwarding of the RREQ. This enables a quicker response to route availability, eliminating unnecessary further flooding of RREQs.

Sequence numbers are used by AODV to identify fresher routing information. Every node maintains its own sequence number, incrementing it before sending either a new RREQ or RREP message. The sequence numbers are included in routing messages and recorded in routing tables. AODV favours newer information, thus nodes update their routing table whenever they receive a message with a higher sequence number (a larger number refers to newer information) or a smaller hop count (smaller hop count refers to shorter path) than what exists in the routing table for a given destination. However, a sequence number is given a higher priority than a hop count. That is, a route with newer information is favoured even if it is longer.

Being a reactive routing protocol, AODV does not give nodes a complete view of network topology. That is, each node only knows its neighbours, and for the non-neighbours, it only knows the next hop to reach them and the distance in hops. However, the security of AODV is compromised by the *Black Hole* nodes, as it accepts the received RREP having fresher route.

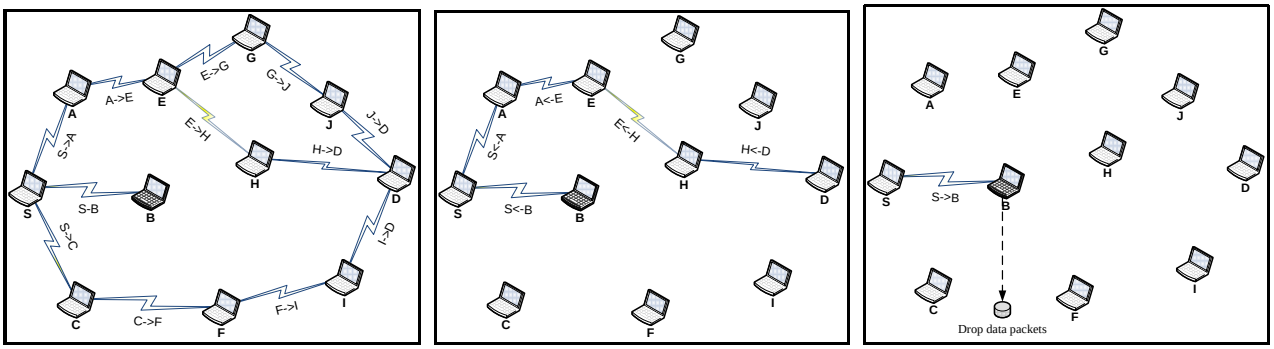
The standard AODV routing protocol cannot fight the threat of *Black Hole* attacks, because during the phase of route discovery, malicious nodes may counterfeit a sequence number and hop count in the routing message; thereby, acquiring the route, eavesdropping or/and dropping all the data packets as they pass.

IV. BLACK HOLE ATTACK

Due to the nature of instances that prompts the use of MANETs such as communication during natural disasters, on the battlefield, and business conferences, there is a need for guaranteed safety of data transfer between two communicating nodes. Thus, secure routing protocols [31, 32, 33, 34] have been recently proposed. Secure routing protocols are mostly designed to prevent hazards to safety properties, such as: (i) identity authentication and non-reputation; (ii) availability of resources; (iii) integrity; and (iv) confidentiality and privacy. A *Black Hole* attack [3, 34] scrambles the route by forging a routing message, and then, further either eavesdrops or drop the packets, posing a possible threat to safety properties (ii), (iii), and (iv). Following *Black Hole* attack easy-to-operate behaviour, it has become a common security threat in MANETs, making it very important to be efficiently prevented.

A *Black Hole* attack forges the sequence number and hop count of a routing message to forcibly acquire the route, and then eavesdrop or drop all data packets that pass. A malicious node impersonates a destination node by sending a spoofed RREP to a source node that initiated a route discovery. A *Black Hole* node has two properties [35]: (1) the node exploits the ad hoc routing protocol and advertises itself as having a valid route to a destination, even though the route is spurious, with the intention of intercepting packets, and (2) the node consumes the intercepted packets. The behaviour of a *Black Hole* attack is depicted in Fig. 1, where a source node S intends to establish a route to destination node D. In AODV routing protocol [8], a source node would broadcast a RREQ packet to establish a route to a destination; with the normal intermediate nodes receiving and continuously broadcasting the RREQ, except the *Black Hole* node. Everything works well if the RREP from a normal node reaches the source node first; but the RREP from *Black Hole* could reach the source node first, if it is nearer to the source node. Moreover, a *Black Hole* node does not need to check its routing table when sending false RREP message; its response is likely to reach the source node first. This makes the source node to conclude that the route discovery process is complete, ignoring all other RREPs and beginning to send data packets. The *Black Hole* node would directly send a route reply (RREP) to the source node S, with an extremely large sequence number and hop count of 1, as shown in Fig. 1(a). The destination node D would also select a route with a minimum hop count upon receiving RREQs from normal nodes, and send a RREP packet as illustrated in Fig. 1(b). Based on the AODV protocol, a source node S would select the latest and shortest (i.e., largest sequence number and minimum hop count) route to send the data packets from the RREPs packets received. It implies that a route via the *Black Hole* node would be selected by node S. The received data packets by the *Black Hole* node will then be eavesdropped or dropped as in Fig. 1(c). Therefore, source and destination nodes are unable to communicate with each other as in [19].

The malicious node always sends RREP as soon as it receives RREQ without performing standard AODV operations, while keeping the Destination Sequence number very high. Since AODV considers RREP having higher value of destination sequence number to be fresh, the RREP sent by the malicious node is treated fresh. Thus, malicious nodes succeed in injecting *Black Hole* attacks.



a) RREQ flooding b) RREP Replying c) Black Hole attack

Figure 1. Diagram of a *Black Hole* attack

V. Related Works Review

Routing algorithms using sequence numbers and hop counts in determining best routes such as AODV [8] and DSR [9] are likely to experience *Black Hole* attacks. Numerous approaches have been proposed in the literature to guard the algorithms against such attacks. The AODV routing protocol was revised in [36] to reduce opportunities for a *Black Hole* node to acquire a route by the source node dropping the first two received RREPs, but selectively picking any subsequent RREP packets. This approach will likely be appropriate in cases where a *Black Hole* node is located nearer to a source node and likely to underperform when it is located many hops away from the source node.

A proposal that a source node waits for a predetermined time value to receive other RREPs with next hop details from the other neighbouring nodes, without sending the DATA packets to the first RREP node at once is presented in [35]. Upon the expiry of the timer, it checks in CRRT table to find out any repeated next hop node. It then assumes the paths are correct or the chance of malicious path is limited if any repeated next hop node is present in the RREP paths. And upon comparison of the received RREPs, selects a neighbour which has the same next hop as other alternative routes to send the data packets. This solution adds a delay and decreases throughput as more RREPs are waited for, and the process of finding repeated next hop is an extra computation overhead.

The PCBHA (Prevention of a Co-operative Black Hole Attack) proposed in [37] is another revised AODV routing protocol aimed at preventing cooperative *Black Holes*. It begins by providing each legal user with a default fidelity level. After broadcasting a RREQ, a source node waits for RREQs from its neighbours and then selects a neighbour with a higher fidelity level, which exceeds the threshold value, for data packets forwarding. The destination node sends an acknowledgement message (ACK) after receiving a data packet and the source node may increase the neighbour's fidelity level by 1, upon receiving the ACK response. A neighbour's fidelity level will be reduced by 1 if no ACK response is received by the source, which indicates a possible *Black Hole* node on the route, which drops data packets before reaching the destination node. The approach works well where the malicious node is not in a position to generate an ACK packet with a faked destination ID. This implies that a source node has to counter check the IDs in the ACK table entities to verify that it is indeed from the destination node. However, the selection of an optimal threshold fidelity level still needs to be determined for accurate detection.

A dynamic learning method intended to detect a *Black Hole* node is proposed in [19]. It observes if the characteristic change of a node exceeds the threshold within a given time period. A node is declared a *Black Hole* node if its characteristic change exceeds the threshold. Otherwise, the latest observation data is added into dataset for dynamic updates. The characteristics observed in [19] are the number of sent RREQs, the number of received RREPs, and the mean destination sequence numbers of the observed RREQs and RREPs. However, no detection mode such as revising the AODV protocol or deploying IDS (Intrusion Detection System) nodes are involved in [19], thus, *Black Hole* nodes are not isolated by this approach. Furthermore, this comes with increased processing overhead and the determination of optimal threshold values remains unresolved.

A routing algorithm based on OLSR (Optimized Link State Routing) [38] to prevent the cooperative *Black Holes* attack, adding two control packets (hop_ACK and HELLO_rep) is proposed in [39]. A survey on *Black Hole* attacks on MANETs with analysed advantages and disadvantages is also presented in [40]. Despite the analysed advantages, *Black Hole* attack remains a security threat.

An attempt to address the survivability problem of the routing service when selective dropping attacks were launched, using trusted nodes to monitor neighbours is presented in [41]. However, the method could not work well in a sparse network where there were no enough neighbours to act as the monitoring nodes. A proposal that each node overhears all traffic of its neighbours and then compares the values observed with some metric to detect abnormal behaviours in the network is made in [42]. The approach requires nodes to be in promiscuous mode and process all overheard packets, which can be energy consuming, impacting negatively on energy

constrained mobile nodes. Furthermore, nodes might not overhear neighbours' transmissions in a sparse network due to insufficient transmission power, which limits transmission ranges.

A ferry based detection method (FBIDM) to detect malicious nodes and mitigate *Black Hole* attacks by introducing a trusted examiner (ferry node) is proposed in [43]. However, the transitive property was not considered when calculating the delivery probability, which is an important property reflecting the encountering of nodes in MANETs. An improved ferry based detection method (MUTON) in which the transitive property was considered, achieving a better detection performance than FBIDM is proposed in [44]. However, MUTON similarly uses trusted ferry nodes in its detection mechanism, thus, requiring additional devices to be deployed in the network, which may not be economical or feasible.

The concept of encounter tickets to secure the evidence of nodes' communication is introduced in [45]. The nodes uniquely interpret the contact history by making observations based on the encounter tickets. However, the method can only prevent the attacker from claiming non-existent encounters, but cannot address the packet dropping in the *Black Hole* attack.

Secure AODV (SAODV) [46, 47] defines a set of message extensions to RREQ, RREP and RERR messages in AODV. New messages also exist for detecting duplicate network addresses. The mechanism provides the authentication of the originator and destination nodes. However, SAODV has weaknesses; nothing prevents a node from increasing a hop count arbitrarily or leaving it unchanged. The latter is similarly identified in [47] as a weakness, since malicious nodes utilize it to attract traffic. The former can also be utilized by malicious nodes, by consistently declaring high hop counts to acquire routes. Further weakness in SAODV is that it does not protect the sender IP address field. A malicious node can impersonate another node while forwarding a RREP to acquire routes.

A solution to *Black Hole* attack based on modification of the AODV protocol is proposed in [3]. The route through the next hop in the agreed upon path is checked. This implies the addition of the next hop information to the standard AODV header. The same approach is adopted in [48], where nodes send their neighbourhood sets once the route is established. Two *Black Hole* attack detection approaches are proposed in [49]: sending a ping packet to the destination to confirm the established route and waiting for the receipt of an acknowledgement, failure of which the presence of a *Black Hole* is deduced; and keeping track of sequence numbers since *Black Holes* usually temper with them, sending packets with unusually high sequence numbers. The former increases delay and traffic overhead.

A dynamic learning system (DPRAODV) which checks to detect the existence of a RREP sequence number (RREP_seq_no) that is higher than the threshold value is proposed in [50]. A node is then suspected to be malicious if its RREP_seq_no is higher than the threshold value, and is added to the black list. The threshold value is dynamically updated at every time interval. A node sends a control packet ALARM, to its neighbours whenever it detects an anomaly. The ALARM packet has the black list node as a parameter, notifying the neighbouring nodes to discard any RREP packet from any suspected malicious node (i.e., no processing is done to the packet). However, the dynamic update of the threshold value at every time interval leads to overheads. Similarly, the determination of an optimal threshold value is necessary for accurate anomaly detection.

A protocol requiring intermediate nodes to send RREP packets containing next hop information is proposed in [3]. A source node receiving a RREP will send a RREQ to the next hop to verify the existence of a route to the RREP generator from the next hop, and another route from the next hop to the destination. When the next hop receives the route verification RREQ, it sends back a further reply to source node with check results. The source node finally judges the validity of the route based on the further reply information. This approach leads to an increased delay and overheads. A proposal in [51] establishes more than one route to verify the authenticity of the RREP initiator. A safe route is determined by the source node if the established routes share same hops. However, it reduces throughput and increases delays in establishing many routes before data transmission.

VI. Simulation Performance Analysis

The simulation is done using OMNeT++ [52, 53] discrete simulator, to analyze the AODV routing performance under the influence of a *Black Hole* attack, by varying the node mobility speed. Simulation parameters are set as shown in Table I.

TABLE I. Simulation Parameters

Parameter	Value
Simulator	OMNeT++
Number of mobile nodes	40
Number of malicious (black-hole) nodes	1
Topology	1500m × 1500m
Transmission Range	250m
Routing Protocol	AODV
Traffic	Constant bit rate (CBR)
Packet size	512 bytes
Pause time	30 (s)
Node mobility model	Random Waypoint model (RWP) [54]

The metrics used to evaluate the performance are as follows:

a) Throughput: it is the total number of received packets per unit time (the ratio of total received packets to total traversing time). That is, the average rates of successful message delivery over a communication channel.
b) Packet Delivery Ratio: it is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source node.

c) End-to-end delay: it is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver (destination). That is, the difference between the receiving time and the sending time. This consists of the delays caused by the buffering and processing at the intermediate nodes.

The effect of a *Black Hole* attack on AODV routing protocol performance were evaluated as follows:

a) Throughput decreases in the presence of a *Black Hole* node in the network as shown in Fig. 2. The analysis shows that throughput is very high in AODV than *Black-Hole AODV* because of higher packet loss in the latter.

b) Packet delivery ratio decreases when there is a malicious (*Black Hole*) node in the network as shown in Fig. 3. This is because some of the packets are dropped by the *Black Hole* node.

c) End-to-end delay decreases in the presence of a *Black Hole* node in the network, as shown in Fig. 4. This is due to the immediate reply from the malicious node, as it does not check its routing table before generating a RREP. However, the decrease in end-to-end delay is of no benefit due to tremendous packet loss as a result of packet dropping by the *Black Hole* node.

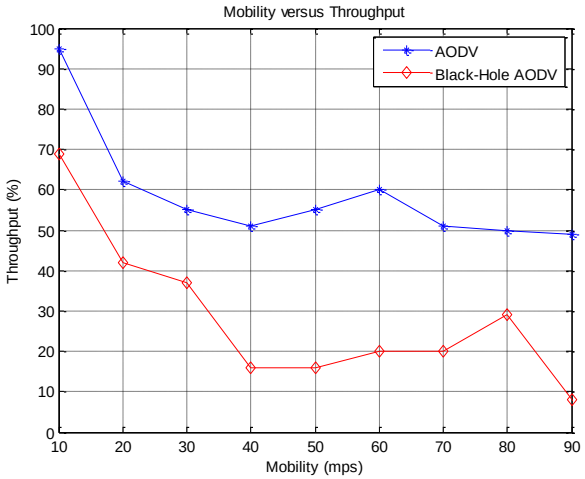


Figure 2. Effect of *Black Hole* Attack on the Network Throughput

VII. CONCLUSION

A *Black Hole* attack is one of the most serious security problems in MANET. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper a survey on secure AODV-based routing in MANET against *Black Hole* attack is presented. The existing solutions affect the AODV performance negatively in terms of throughput, delay and overheads. Although these may not be avoided in totality, there is a need for trade-offs to achieve a secure optimal performances. One of the suggested approaches for improvement is to determine optimal threshold values for accurate anomaly detections. Solution approaches that result in further traffic congestion should be least considered.

Based on the above performance comparisons, it can be concluded that *Black Hole* attacks affect the AODV routing protocol negatively. Hence, there is need for 'perfect' detection and elimination mechanisms.

The detection of *Black Holes* in ad hoc networks is still considered to be a challenging task. Future work is intended to an efficient *Black Hole* attack detection and elimination algorithm with trade-offs in delay and overheads that can be adapted for ad hoc networks susceptible to *Black Hole* attacks.

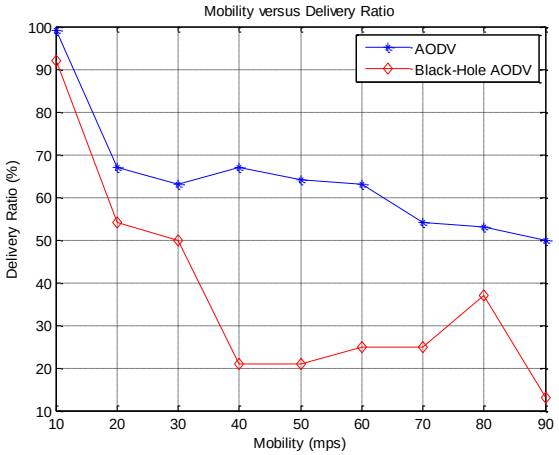


Figure 3. Effect of *Black Hole* Attack on the Network Packet Delivery Ratio

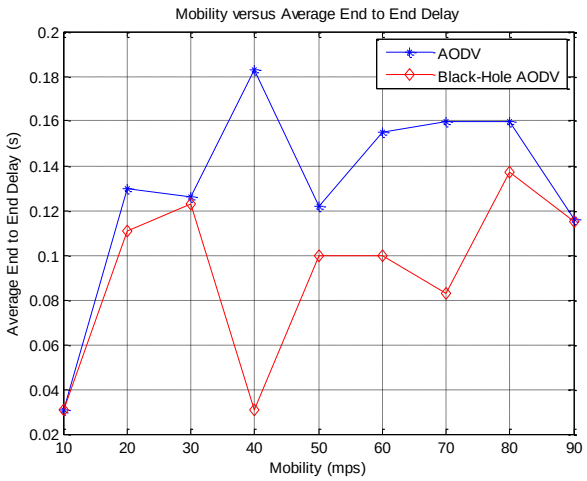


Figure 4. Effect of *Black Hole* Attack on the Network Average End to End Delay

REFERENCES

[1] Poongothai T. and Jayarajan K., "A non-cooperative game approach for intrusion detection in Mobile Adhoc networks", International

Conference of Computing, Communication and Networking (ICCC), 18-20 Dec 2008, St. Thomas, VI, pp 1-4

[2] Charles E. Perkins, "Ad Hoc Networking", Addison- Wesley, Pearson edu., Jan. 2001.

[3] H. Deng, W. Li, and Dharma P. Agrawal, "Routing Security in Ad Hoc Networks, "IEEE Communications Magazine, Special Topics on Secuity in Telecommunication Networks, October 2002

[4] Latha Tamilselvan and Dr. V.Sankaranarayanan, "Solution to Prevent Rushing Attack in Wireless Mobile Ad hoc Networks", Ad Hoc and Ubiquitous Computing, December 2006, pp. 42-47.

[5] Hongmei Deng, Wei Li, and Dharma P. Agarwal "Routing security in wireless Ad Hoc networks" IEEE Communications Magazine, October 2002.

[6] Charles E. Perkins, Pravin Bhagwat, Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers, SIGCOMM (1994).

[7] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003.

[8] C.E. Perkins, E. Beliding-Royer, S. Das, Ad hoc on-demand distance vector (AODV) routing, IETF Internet Draft, MANET working group, Jan. 2004.

[9] D.B. Johnson, D.A. Maltz, Y.-C. Hu, ''The Dynamic Source Routing Protocol for Mobile Ad-hoc Network (DSR)," IETF Internet Draft, July 2004.

[10] Yi-Chun Hu, Adrian Perrig, David B. Johnson "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", WiSe 2003, September 19, 2003, San Diego, California, USA.

[11] Lidong zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue, November/December 1999.

[12] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy May/June 2004.

[13] Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, "Routing Security in Ad Hoc wireless Networks", Network Security, 2005 Springer.

[14] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," *Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps.*, New Orleans, LA, Feb. 1999, pp. 90–100.

[15] J. Schiller, "Mobile Communications", Addison-Wesley, Pearson education August 2003.

[16] F. Anjum, Anup K. Ghosh, nada golmie, paul kolodzy, radha poovendran, rajeev shorey, d. Lee, *j-sac, "Security in Wireless Ad hoc Networks*", ieee journal on selected areas in communications, vol. 24, no. 2, February 2006.

[17] H.-A. Wen, C.-L. Lin, and T. Hwang, "*Provably Secure Authenticated Key Exchange Protocols for Low Power Computing Clients*," Computers and Security, vol. 25, pp. 106-113, 2006.

[18] Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "*Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*" In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003.

[19] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, issue 3, Nov 2007, pp 338–346.

[20] Yuh-Ren Tsai, Shiuh-Jeng Wang, *"Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks"* Chung-Shan Institute of Science and Technology, Taiwan, R.O.C., under Grant BC-93 B14P and the National Science Council, Taiwan, R.O.C., IEEE 2004.

[21] Karan Singh, R. S. Yadav, Ranvijay, "A Review Paper on Ad Hoc Network Security", International Journal of Computer Science and Security, vol. 1, no. 1, February 2010

[22] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, *"Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04*, April 2-3, 2004, Huntsville, AL, USA.

[23] K. Balakrishnan, J. Deng, and P.K. Varshney, "*TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks"* Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

[24] Patroklos g. Argyroudis and donal o'mahony, "*Secure Routing for Mobile Ad hoc Networks*", IEEE Communications Surveys & Tutorials Third Quarter 2005.

[25] I. Aad, J.-P. Hubaux, and E-W. Knightly, *"Denial of Service Resilience in Ad Hoc Networks,"* Proc. MobiCom, 2004.

[26] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" *WiSe 2003*, September 19, 2003, San Diego, California, USA.

[27] Akanksha Saini, and Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET", International Journal of Computer Science and Technology, Vol.1, issue 2, Dec 2010

[28] Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and Kashyap Balakrishnan, Member, IEEE, "*An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs"* IEEE Transaction on Mobile Computing, VOL. 6, NO. 5, May 2007

[29] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[30] Davide Cerri and Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype," IEEE Communications Magazine, February 2008

[31] Manel G. Zapata, N. Asokan, ''Securing Ad-hoc Routing Protocols", in: Proc. of the ACM Workshop on Wireless Security (WiSe), 2002.

[32] Kimaya Sanzgiri, Bridget Dahill, Brain Neil Levine, Clay Shields, Elizabeth Belding-Royer, ''A Secure Routing Protocol for Ad hoc Networks", in: Proc. of the IEEE International Conference on Network Protocols (ICNP'02), November 2002.

[33] Yih-Chun Hu, Adrian Perrig, David B. Johnson, ''Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", in: Proc. of the ACM Conference on Mobile Computing and Networking (MobiCom), pp. 12–23, 2002.

[34] Ming-Yang Su, ''Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications, vol. 34, pp. 107-117, 2011.

[35] Latha Tamilselvan, Dr.V Sankaranarayanan, "Prevention of Blackhole Attack in MANET". The 2nd International Conference on Wireles Broadband and Ultra Wideband Communications (AusWireless 2007) India, 2007 IEEE.

[36] Semih Dokurer, Y.M. Erten, Can Erkin Acar, ''Performance Analysis of Ad-hoc Networks under Black Hole Attacks", in: Proc. of the IEEE SoutheastCon, pp. 148–153, 2007.

[37] Latha Tamilselvan, Dr.V. Sankaranarayanan, Prevention of co-operative black hole attack in MANET, Journal of Networks 3 (5) (2008) 13–20.

[38] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003.

[39] Soufine Djahel, Farid Nait-Abdesselam, Ashfaq Khokhar, ''An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol", in: Proc. of the IEEE International Conference on Communications (ICC), pp. 2780–2785, 2008.

[40] R.A. Raja Mahmood, A.I. Khan, ''A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks", in: Proc. of the International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET), pp. 1–6, 2007.

[41] S. Marti, T.J.Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *6th ACM International Conference in Mobile Computing and Networks*, August 2000.

[42] Y.Huang and W.Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proceedings of 1st ACM Workshop on Security of Ad Hoc Networks*, 2003.

[43] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected adhoc networks," in *Proceedings of first workshop on security for emerging ubiquitous computing*, 2007.

[44] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Muton: Detecting malicious nodes in disruption-tolerant networks," in *WCNC 2010*, 2010.

[45] F. Li, J. Wu, and A. Srinivasan, "Thwarting black hole attacks in distruption-tolerant networks using encounter tickets," in *Infocom 2009*, 2009.

[46] M. G. Zapata, "Secure ad hoc on-demand distance vector (SAODV) routing," Internet Draft, draft-guerrero-manet-saodv-06, work in progress, September 2006.

[47] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *the ACM Workshop on Wireless Security (WiSe'02)*, 2002.

[48] Lidong Zhou, Zygmunt J.Hass, "Securing Ad Hoc Networks*", IEEE Special Issue on Network Security*, vol-13, pp 24-30 Nov-Dec 1999

[49] P.Ning and K.Sum, "How to misuse AODV: A case study of insider attack against mobile ad hoc routing protocol", Tech Rep, TR- 2003-07, CS Department, NC University, April 2003

[50] Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet", International Journal of Computer Science Issues, Vol. 2,pp 54-59,2009.

[51] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks", in *ACM 42nd Southeast Conference (ACMSE'04)*, pp 96-97, Apr. 2004.

[52] Andrias Vraga, OMNeT++, www.omnetpp.org.

[53] A. Varga, OMNET++, in the column "Software Tools for Networking," *IEEE Network Interactive, 16*, 4, July 2002

[54] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," IEEE Transactions on Mobile Computing, vol. 2, no. 3, pp. 257-269, Jul./Sep. 2003.