Journal of Computer Science

Original Research Paper

A Comprehensive Review and Performance Evaluation of Detection Techniques of Black Hole Attack in MANET

Sunil Kumar Jangir and Naveen Hemrajani

Department of Computer Science and Engineering, JECRC University, Jaipur, India

Article history
Received: 13-06-2017
Revised: 20-09-2017
Accepted: 11-10-2017

Corresponding Author:
Sunil Kumar Jangir
Department of Computer Science and Engineering, JECRC University, Jaipur, India
Email: sunil.jangir07@gmail.com

Abstract: Mobile Ad Hoc Network (MANET) is an auto Configuring network. Due to its natural characteristics, a MANET is vulnerable to many security threats. Blackhole attack compromises the performance and the reliability of the network. Since nodes are allowed to move freely within the network, it becomes very important to protect the communication among mobile nodes for the sake of security. In this paper we have investigated various techniques that can detect Blackhole attacks in MANET and we have compared the detection techniques with different matrices such as Average Packet Delivery ratio and Average End-To-End delay.

Keywords: MANET, Black Hole Attack, Denial-of-Service

Introduction

Ad hoc networks are not centralized and are wireless networks. They are infrastructure less networks, suitable for situations where setting an infrastructure is either not feasible or is costly. Mingyan *et al*. (1999), a mobile Ad hoc Network is dynamic in nature and in such a network nodes are allowed to move freely during the communication. Nodes that are not in each other's vicinity, communicate with multi hop communication. Due to its characteristics the network is vulnerable to many security attacks and it is used in places where infrastructure networks do not work well like battle field, disaster management etc Sakshi (2014).

MANET security attacks are classified into Active Attack and Passive Attack. In a passive attack, the assault is not intended to destroy the operation of the protocol but to reveal the information of the network. An attacker may not change any message in passive attack. In an active attack, the messages may be modified by the attacker, however these attacks generally involve actions performed by various adversaries, modification of transmitted data, deletion of transmitted data etc. Attacks like impersonation, disclosure and Denial of Service attack are known as active attacks.

Impersonation

In impersonation first the assaulting node slips into the network by donning the identity of some other node and then transmits false routing information.

Disclosure

In disclosure the attacker node discloses the location information about the target node.

Denial of Service (DoS) Attack

In DoS attack, the attacker jams the network or overflows the routing table of the target node and continues to send false routing information (Radhika and Wandra, 2015; Panagiotis and Haas, 2002; Hu *et al*., 2002; Semih *et al*., 2007; Wu *et al*., 2007).

Blackhole Attack

Blackhole attack is a prime security threat in MANET. In a black hole attack, an as assaulting node utilizes the protocols and misguides by revealing a shortest path to the desired node. But instead of forwarding the packets to its neighboring node, the malicious node eventually drops routing packets (Perkins and Royer, 1999; Maan *et al*., 2011)

A blackhole assailant first assaults into the multicast forwarding group by instigating a rushing assault, keeping in mind the end goal of capturing the information group of the multicast session. The aggressor drops a few or the majority of the packets that it gets as opposed to sending the packets to the following nodes on the route. This sort of assault frequently brings about low packet delivery ratio Hoang and Uyen (2008).

Ad hoc On-Demand Vector routing (AODV) protocol is probably the most famous MANET routing protocol. This protocol offers several benefits such as dynamic, self starting and multihop routing.

Furthermore, it is able to adapt MANET topology changes and can automatically reject the inactive routes, Perkins and Royer (1999).

Sadly, AODV is prone to many routing assaults. (Maan *et al*., 2011; Ramaswamy *et al*., 2003).

Blackhole attack is the one of the most severe attacks in AODV-based MANET, Ramaswamy *et al*. (2003). In this assault false routing data is produced by the assailant and it is sent to the casualty nodes to cause false route entries in the routing tables of the nodes. Accordingly, numerous erroneous routing exist and cause bottleneck in the communication channels. Steering Protocols There are various directing conventions in MANET. In this segment, we will examine a portion of the renowned steering conventions.

Routing Protocols

MANET has a long list of routing protocols. In the following section, we will be discussing some of the routing protocols. Since the current routing information is not known so for that purpose prior communicating with a target node, the mobile node should broadcast its present status to the neighbors.

Routing protocols are classified on the basis of how the information is acquired. In the below classification we are going to discuss:

- Proactive Routing Protocol
- Reactive Routing Protocol

Proactive (Table-Driven) Routing Protocol

The alternate identification for this protocol is table-driven routing protocol. In proactive routing protocols, routing information is broadcasted to the neighbours. Every node keeps a routing table to keep a list of the adjacent nodes, reachable nodes and the number of jumps required. Thus every node has to evaluate the neighbourhood as long as the network topology is changing.

Hence there is a disadvantage of overhead rise because as the size of the network increases, communication overhead within a larger network topology also increases. Nonetheless, there is favorable position that the network status can be instantly reflected if any pernicious node joins the system. The Destination Sequenced Distance Vector (DSDV) Tseng *et al*. (2011), routing protocol and Optimized Link State Routing (OLSR) protocol are some of the well known routing protocols Royer and Toh (1999) protocol (Ramaswamy *et al*., 2003; Deng *et al*., 2002).

Reactive (on-demand) Routing Protocol

A reactive routing is actualized with on-request routing conventions. In opposition to the proactive routing that communicates the routing information; the reactive routing is just started when nodes want to transmit the information packets. A noteworthy preferred standpoint of this methodology is that there is a decreased wastage of data transfer capacity that is initiated from the cyclic broadcast. The shortcoming of these conventions is that passive routing technique prompts some packet loss. Here we quickly portray two renowned on-request routing protocols i.e. Ad hoc on-demand Distance Vector (AODV) Sanzgiri and Dahill (2002) and Dynamic Source Routing (DSR) Perkins and Bhagwat (1994) protocol.

In AODV, every node just records the following hop data in its routing table but keeps it for maintaining a routing way from source to destination node.
If the target node can't be reached from the source node then a route discovery process will be initiated shortly.

Security Criteria

Earlier, encryption and firewalls were used to protect the network which did not prove much efficient for a MANET infrastructure, for the major concern in MANET security is integrity, authentication, confidentiality, non-repudiation, availability to mobile users and anonymity as described below.

Availability

Zhou and Haas (1999) Availability maintains the activeness of the network despite various attacks. Its major concern is the unauthorized and illegal access of resources. In some attacks, there could be possible disruption of routing protocol and continuity of services in the network.

Confidentiality

Confidentiality ensures protection from passive attacks. In military, the leakage of information can't be compromised. Confidentiality ensures authorized access of information that protects data. Even it ensures the confidentiality of router location and packet information.

Authentication

Zhou and Haas (1999) Authentication ensures that communicating parties are authorized parties by verifying their identity before communication. Ubiquitous networks need mutual authentication and for mutual authentication, a mutual authentication protocol is necessary to prevent the attacks.

Integrity

Integrity guarantees that message delivered is neither modified nor duplicated or reordered for replay of original message. It also ensures that only the authorized parties retrieve the information or messages and the message is not corrupted or lost. Integrity ensures that messages are delivered to the authorized parties as sent.

Nonrepudiation

Nonrepudiation makes sure that sending node can't challenge its previous communications. It can always be proved by the receiver that a particular message was sent by an alleged sender. It can also be used for isolation and detection of nodes.

Scalability

Although the security is not affected by the scalability directly but as the network may consist of hundreds or thousands of nodes and if the network is not scalable enough then new nodes cannot be added to the network. The attacker thus may compromise the newly added nodes and get access to the network.

Anonymity

This simply helps in ensuring the privacy of the personal information about the owner or user and it is not disclosed by the node.

Detection Techniques

Sukla (2008) proposed a mechanism that is able to remove and detect the malicious nodes. This approach comprises of an algorithm that as opposed to sending complete traffic information at a single purpose of time, send the traffic data in some little estimated blocks. In this way by guaranteeing an end-to-end checking, all the attacker nodes can be detected and evacuated in the middle of the transmission of two such little blocks. Before transmitting a response to any node, the initiating node sends a prelude messages to the target node to alert it about the upcoming information piece.

Traffic movement is observed by the neighboring nodes in the course. Destination node sends an acknowledgment after the finish of the transmission by means of a postlude message containing the aggregate number of information packets got by the destination node.

This information is further checked by the source node to see if the data loss is in tolerable range or not. If the data loss is very high then the process of detection is initiated and the malicious node is removed by aggregating the responses from the network and monitoring the contributing nodes.

Satoshi *et al.* (2007) proposed an anomaly detection technique that utilizes dynamic preparing strategy in which the preparation information is refreshed at standard interim of time where the Multidimensional component vector is recognized to express state and status of the network of every node. According to us here each dimension is counted on every time slot. It utilizes sequence number of the destination to identify assault. The feature vector likewise incorporates number of RREQ messages sent, number of RREP messages received and the normal of contrast of destination sequence number in each availability between succession number of RREP message and the one held in the list. Here mean time is figured by computing some numerical count. There is an assault when the separation is more prominent than some threshold value.

Shalini (2010) proposed a technique based on sending of data in terms of small packets of equal sized blocks instead of sending the complete data in one continuous flow. According to us in this technique the message flow is monitored independently at both source and destination node. The checked outcome is accumulated by the spine network of trusted nodes. As per result every node can locally keep up their own particular table of malicious or boycotted nodes and at whatever point a malicious node endeavors to send information to any genuine node, it can likewise caution the system about the malicious or boycotted nodes. This list of malevolent nodes might be utilized to find secure ways from source node to destination node by maintaining a strategic distance from various black nodes acting in participation.

Anishi (2013) has proposed MEAODV (Modified Enhanced AODV) that depends on the past work of EAODV (Enhanced AODV). According to our survey and study, the MEAODV depends on route discovery procedure to relieve the impacts of the black hole assaults. It has couple of various condition parameters for checking the RREP messages for better course disclosure system however has a comparable rationale as in EAODV. In simulation, by fluctuating nodes, it offers preferable PDR over EAODV. It can be reasoned that MEAODV has remarkable outcomes as far as better Performance Delivery Ratio (PDR) and less End-to-End Delay as contrast with EAODV strategy.

Sanjay *et al.* (2013), with the control packets called CONFIRM, CHCKCNFRM and REPLYCONFIRM, they have effectively distinguished the nearness of Black Hole and thus effectively occupied all the traffic from it. According to our study, here even a slight modification in the protocol shows that how single run of the algorithm can detect the presence of collaborative Black Hole chains. They were also able to detect time varying and target varying Black Holes called the gray Holes with slight modifications in our method which produces 90 percent DDR for dynamic topology with an end to end delay, 0.9 times greater than that of conventional AODV. So, simulation results also show that algorithm is packet traffic efficient as well as time efficient.

Rutvij (2013) have investigated on many existing approaches on how to tackle Blackhole and Grayhole attacks and have discussed their previous work. Here they have presented the slightly altered improved protocol viz. MRAODV which is based on their previous work viz. R-AODV that removes the limitations in the existing mechanisms. According to us in the purposed approach during the route discovery phase MR-AODV isolates Blackhole and Grayhole nodes as R-AODV and sets up a new secure route to send the data. It attempts to lessen the normalized routing overhead by diminishing the number of forwarded reply packets which are sent by the adversary nodes. A simulation result which has been presented in form of graphs proves that the MR-AODV is the reliable solution which under various network parameters and traffic conditions gives the considerable enhancement in PDR with acceptable average end-to-end delay and normalized routing overhead.

Sakshi and Khuteta (2015), researchers proposed a modification on Ad-hoc On Demand Distance Vector (AODV). In this AODV act like a self initiating routing protocol for MANETs. According to us in this purposed mechanism the security of this protocol is degraded with a particular type of attack know as "Blackhole" attack. In such type of attack the malicious node advertise itself as having the best path to destination while discovering route therefore interrupt the real communication and degrade network performance. In the proposed plot it has been conveyed that the base node in the system that builds the likelihood of distinguishing different vindictive nodes in system and further disconnect them from participating in any correspondence.

Vaishali and Lata (2015), to maintain a strategic distance from single blackhole attack in MANET. According to us they have considered a component that utilizations further Route Request packets. For distinguishing and evading agreeable blackhole attack they propose another method which utilizes Cooperative Cluster Agents. In this particular scheme they pass DRI and SRT-RRT tables as a contribution to Cooperative Security Agents. In view of these sources of info the CSAs utilize cross checking and location stream instruments for recognizing helpful blackhole attack, once it is identified that can be maintained a strategic ca can be maintained distance from by passing ready warning in the MANET. For execution of the proposed conspire they will utilize organize test system - ns-2.35 the proposed arrangement and contrast it and standard AODV protocol as far as throughput, packet delivery ratio and end-to-end delay.

Ayesha *et al.* (2015) in investigated scheme, each and every node in the network environment entertains its neighboring hopes promiscuously. According to us here in promiscuous mode, every node monitors the packet being forwarded by its neighbors in order to observe the behavior of neighbor regarding packet operation. Every node compares the neighbor information with the information it stores in its knowledge table. If both are same the node assumes that the packet is forwarded further, otherwise node waits for particular amount of time and checks the reasons for packet dropping. In order to confirm packets are sent to its neighbor, the nodes monitor the control packets as well as data packets to prevent selective dropping, as black hole attack drops selected packets. In order to monitor the forwarded packets, every node has to maintain knowledge tables with following entries: Fm, rm if the values differ, the nodes are black hole nodes. A secure knowledge algorithm for mitigating black hole attack in AODV protocol has been recommended. The algorithm monitors the data packets that are being forwarded in promiscuous mode to ensure that the packets are delivered to destination node. If any node drops a packet our algorithm checks for the packet drop reasons first before declaring it as a black hole node, thereby preventing a trusted node to act as if it is a blackhole node.

Mohamed and Peter (2016) presents another idea of Self-Protocol Trustiness (SPT) in which distinguishing a pernicious interloper is refined by consenting to the ordinary convention conduct and baits the malevolent node to produce an acknowledgment of its malignant conduct. According to us in this proposed idea a Blackhole Resisting Mechanism (BRM) oppose such attacks that can be consolidated into any responsive directing convention has been proposed. Which doesn't require costly cryptography or confirmation instruments, yet depends on privately connected timer and thresholds to group nodes as pernicious. No changes to the packets configurations are required, so the overhead is a little measure of computation at nodes and no additional correspondence.

Thi and Yeo (2016) for identifying the individual bad conduct, they characterized sending proportion metrics that can recognize the behaviors of assailants from typical nodes. According to us in this the malevolent nodes may abstain from being distinguished by conniving to control their sending proportion metrics. To constantly drop messages and advance the metrics in the meantime, aggressors need to make fake experience records habitually and with high manufactured quantities of delivered responses they misuse the anomalous example of appearance recurrence and number of sent messages in fake experiences to outline a vigorous calculation to identify intriguing aggressors.

Jitendra and Vinit (2014) proposed a novel cluster situated idea is proposed to improve security and proficiency of the system. According to us in this procedure safeguards the ideal execution of MANET in nearness of dark opening attack. The reenactment of the proposed technique is completed utilizing NS2 organize test system and the simulation results reflects the performance of scheme for detection and deterrence for the attack blackhole.

Arun (2016), proposed a mechanism on MANET or Mobile Ad-Hoc Networks that are self-forming systems which do not require a settled framework for its communication. According to us in this mechanism the MANET is assumed as a basic part in Military

Communication and Disaster Management framework. At first there will be different nodes with discrete address relegated from an address pool, which will frame the system when required. The typical security components like encryption and confirmations have no enormous parts in these sorts of attacks. The paper talk about the FPGA execution of black hole warm hole recognition and avoidance algorithm. The packets from a black hole or worm-hole are detected in the MAC-Physical layer itself by arbitrarily changing the Packet Travel Time (PTT). The Mac layer and the physical layer are actualized using Partial-Reconfiguration procedure so that the symbol rate, modulation scheme and coding rate can be changed haphazardly while the framework is running without utilizing additional equipment. Probe request and probe reaction messages are utilized to guarantee verification for the nodes for shaping the system.

Rathiga and Sathappan (2016) in this hybrid approach, the initiated monitor nodes gather the bundle stream information about the neighboring nodes. According to us in this hybrid approach at the point the distance metric is registered utilizing which two location thresholds are resolved. Distance metric for all the nodes is compared with very first threshold. On the off chance that the distance metric of a node is more noteworthy than the principle threshold, then the node is thought to be malevolent nodes. On the off chance that the distance metric of the nodes are beneath the second threshold but not less than principal threshold, the nodes are set apart as grey hole assailants while in the event that they are more noteworthy than the second threshold, the nodes are set apart as black hole aggressors. Exploratory outcomes demonstrate that the proposed hybrid black/grey hole detection approach recognizes and wipes out the attacks adequately with better throughput, packet drop rate, packet delivery ratio and routine overhead.

Neha and Anand (2016) Black-hole and gray-hole attack is one sort of attack which damages and attacks on MANET. According to us According to us in this attack the malevolent (undesirable node) occupy the information packets that it feels is having most brief and the freshest course to the goal node so sender advances every one of the information packets to it. In the wake of getting the information packets, it drops them to make a Denial of administration attack or procedures to concentrate data from the packet. Here a method is being proposed for identification of the black-hole or malicious node. In this strategy, another system a sort of trap technique is included in AODV protocol for the recognition of malignant nodes. At the point when the Black-hole node is distinguished after that a disturbing strategy is activated to make different nodes mindful of vindictive nodes.

Countermeasures

The primary distress in MANET is the safety of communication and soundness of information. A network may have one or more vulnerabilities which can be exploited by an action called attack. It is necessary in network to perform routing and packet forwarding. Several detection techniques have been devised to reduce the effect of the assaults on the environmental paradigm. Preventive and Reactive mechanisms are the type of mechanisms that are used for the protection of MANET.

Mitigation Techniques against Black Hole Attack

The Network Layer are more likely to be exploited as this layer is more vulnerable for attacks than any layer in MANET. Various security threats are imposed on this layer Sanzgiri *et al*. (2002). For the security maintenance, one way is to use the secure routing protocol. Source authentication is used to evoke the routing responses. The Message Authentication Codes (MAC), Digital signatures and Hashed MACs (HMAC), these approaches are used to maintain security at some predefined level. By the use of IPSec, security can be achieved at the network layer in internet. Authenticated Routing for Ad-Hoc Networks (ARAN) is one more additional routing protocol which gives the security and shelter from Blackhole attacks. This routing protocol is used where there are a number of threats and possibilities of change in sequence number, hop count modification and change in source routing and mockery of target addresses Deng *et al*. (2002).

Mitigation Approach by Deng

This approach makes some changes in the AODV protocol to avoid the blackholes. This approach is used for identification of the existence of the advertised Route of the black hole by appending in Route reply (RREP) packets of the intermediate node by their position of the near to next node. After encountering the route reply (RREP) packet from a transitional node, source node collects the information of the next hop node and sends supplementary request to the one jump node for checking the routing metric value with the one jump node. For confirming the route information next hop node of neighbor sends back the supplementary reply packet to the sender. In case the source does not get back this supplementary reply, it specifies that the route contains the malicious nodes. This route is dropped from the distinct routing table and an alarm signal is forwarded to other side nodes in the environment to isolate malicious nodes. The limitations of this policy is that cooperative black hole attacks can be initiated on it. Furthermore, this solution causes additional routing overhead due to supplementary request and supplementary reply for verification.

Mitigation via Destination Sequence Number

The investigated approach by Mistry *et al*. (2009) gives the approach that source node verifies the RREP destination sequence number by analyzing the RREP messages which arrive within the fixed and an unequivocal time period. If sequence number is found to be greater than desired, then the initiating node of the respective RREP will be identified as malicious node due to the high sequence number. The major issue in this method is the latency time during the route discovery process. Before the process of routing table modernization the source node has to halt until the limit of time period is crossed. The node still suffers from the latency even if there is no attack in the network.

Mitigation by Securing Routing Table Update

Kamarularifin *et al*. (2011) have suggested novel called ERDA by analyzing the limitation of lastly advocated policies. ERDA is used to perceive, prevent and segregate the Black hole nodes in MANET. They have shown that ERDA enhances existing function recvReply() in the AODV protocol by implementing a simple mechanism to detect and isolate malicious nodes and improving the process of updating routing entry. The enhancement of this only involves minimum modification to existing AODV protocol flows. Moreover, ERDA does not incur high and delay overhead (Delay) and routing overhead (NRL).

Mitigation by Using Optimal Path Routing and Hash

Hizbullah *et al*. (2013) A trivial moderation in AODV can elude the blackhole attack. In this technique, the sender node originally works as per the AODV routing protocol. It sends Route Request (RREQ) from initiating node to terminating node. As soon as the destination node or intermediate nodes receive the Route Request (RREQ), they send back Route Reply (RREP) messages on the same route from which they have received the RREQ messages by the previous node or the source node. Also for the avoidance of black hole the first RREP message coming from intermediate node is always discarded when the source node sends RREQ to the neighbour node. Here, the second shortest route is preferred over the first shortest route for the transmission of the packets and data. This solution presents the prevention of the network from attack called black hole by using the second shortest path for sending packets to destination. It would not be easy for black hole or grayhole node to monitor the entire network topology and examine where to place themselves in the network and mislead the source node that it has the second shortest route node to the destination. The attack can comfortably be ignored by using this technique as the affected node was not in practice for sending RREP message of the second shortest route to the source node as the malicious node usually generates the RREP message of high sequence number to be treated as the first shortest route node.

Time-Based Limen Mitigation Detection Mechanism

Tamilselvan *et al*. (2007) gives the solution for the detection of black hole and ensuring the reliability of the route before sending the data packets over it. This solution provides the modification of AODV protocol for obtaining the desired goals as follows: The source node does not start sending data packets immediately after awarded the RREP message from any middle ware node. It ensures the safe route for sending data packets by waiting to receive the RREP messages from other neighboring nodes. A timer is then set by the source node for collecting the RREP messages from the neighbouring nodes and maintaining a table for all the received RREP messages. When the times get over, source node is considered and selects the most reliable route for packet transmission which contains the more repeated common nodes from the table. If no repeated common nodes are found, then the source node considers the route which provides information about its next hop in the route. It has a drawback of processing delay and wait strategy for waiting for the reply from neighboring node.

Simulation and Results

The Simulation is performed via NS-3 Network Simulator and the Table 1 summarizes all the simulation parameters.

In G-AODV with the help of control packets called CONFIRM, CHCKCNFRM and REPLYCONFIRM and has diverted traffic from it. MRAODV, ADHOC routing are prone to various attacks such as DoS attack. This is only due to ignorance of security aspect during their designs. MEAODV migrates the black hole attack by controlling the routing update with new condition, parameter and removing the redundancy in detecting malicious nodes. TAPPING-AODV gives the facility to choose the best solution for the routing protocol and also provides the knowledge on how to use those schemes in any environment.

Table 1. Simulation parameters

Parameter	Value
Area	1000×1000
Simulation time	100sec
MAC	802.11
Application traffic	CBR
Routing protocols	AODV,
Pause time	0.5sec
No. of malicious nodes	2-10
Bandwidth	2Mbps
Data payload	512 bytes/packets
Maximum speed	10-50m/s
No. of nodes	100

Average Packet Delivery Ratio is the mean proportion of the received data packets by the receiving node and the total number of packets prompted by the source node. Here in the Fig. 1 as the number of Malicious nodes increase PDR of standard AODV under all parameters starts declining. There is very sharp decline in TAPPING-AODV, the performance of G-AODV is better than the TAPPING-AODV as the decrease in PDR, also the performance result shows that G-AODV performance is slightly low as compared to MR-AODV. There is very small decrease in PDR in MR-AODV as it does not breakout under attack and isolates all the malicious nodes and its performance is better than the other four and gives approx 87% PDR in this case.

Average End-to-End Delay refers to the average time taken to transmit packet from source node to destination node. Here in this figure we can observe that there is an increment in the end-to-end delay as the number of malicious nodes rises in the network. This is because when the packets are transmitted from the source node to the destination node, whenever malicious nodes are found, an algorithm is called either to drop that packet or to start the packet transmission right from the initial state. This ingest time period whenever a malicious node is countered, emanating in a swelled average end-to-end delay. In Fig. 2 we can conclude that the average ETE Delay is increasing in all. Tapping AODV has the maximum ETE Delay than other four and MR-AODV has the minimum ETE Delay than all the other four.

Average Throughput is the total amount of packets successfully transmitted from source node to destination in a particular time. In Fig. 3 we can see that the average throughput is decreasing as the number of malicious node is increasing. Here we have concluded that the BHAODV (Black hole AODV) attack has the minimum throughput. This is because a large amount of packets are dropped during the transmission of packets, so in this attack the number of malicious nodes in the network increases which shows considerable increment in dropping of packets. MRAODV and MEAODV detection technique has the maximum Average throughput which indicates that these two detection technique is the best among all when we use this technique because there is very less packet drop.

Detection Rate is the ratio of the total number of nodes attacked to the total number of attacks in the network that have been detected.

$$Detection\ Rate = \frac{No.\ of\ Detected\ Attacks}{Total\ Attack}$$

In the Fig. 4, it can be seen that there is an increment in the detection rate as the number of malicious nodes increases. The probability of detection of attack increases as the size of the blackhole increases. Tapping AODV detection technique has the least detection rate which shows it is not capable of detecting the attacks on node on large scale. MEAODV and MRAODV has the highest detection rate i.e. they are capable of detecting the maximum attack in the network.

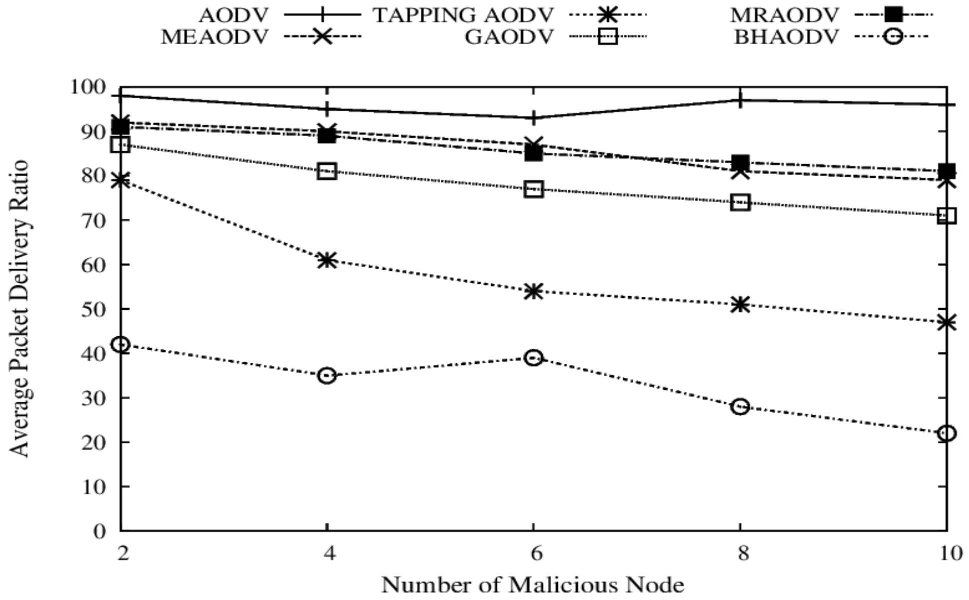

Fig. 1. Average packet delivery ratio for various detection techniques

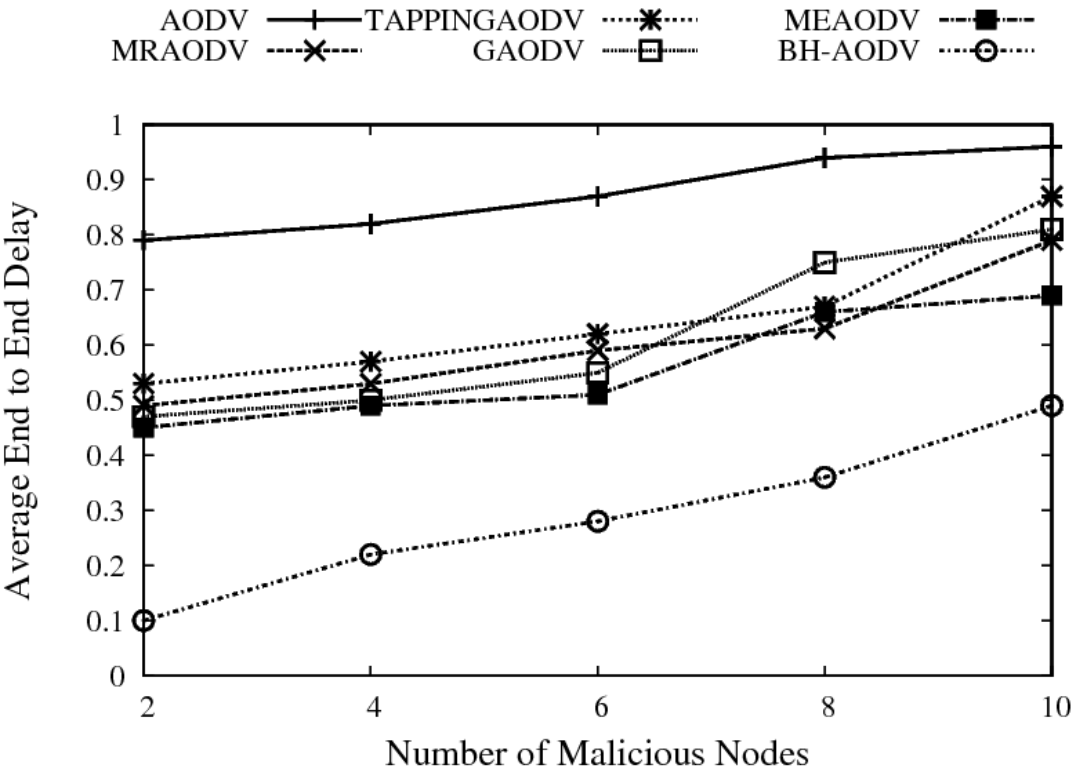

Fig. 2. Average end to end delay for various detection techniques

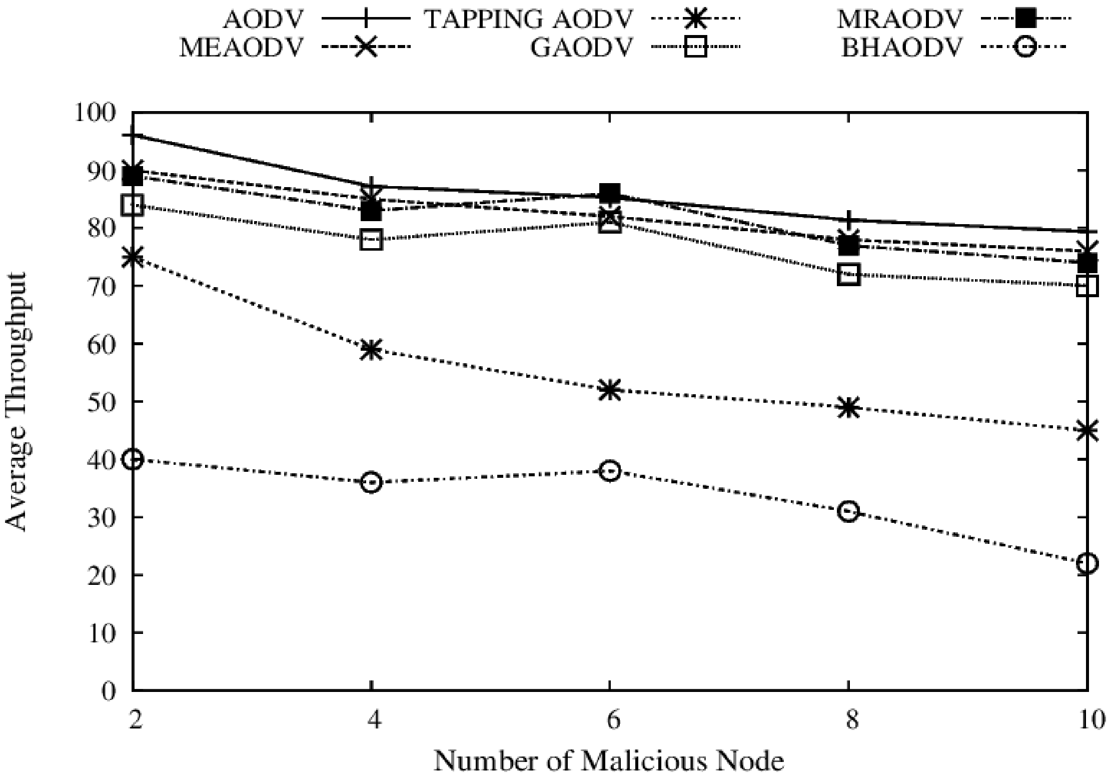

Fig. 3. Average throughput for various detection techniques

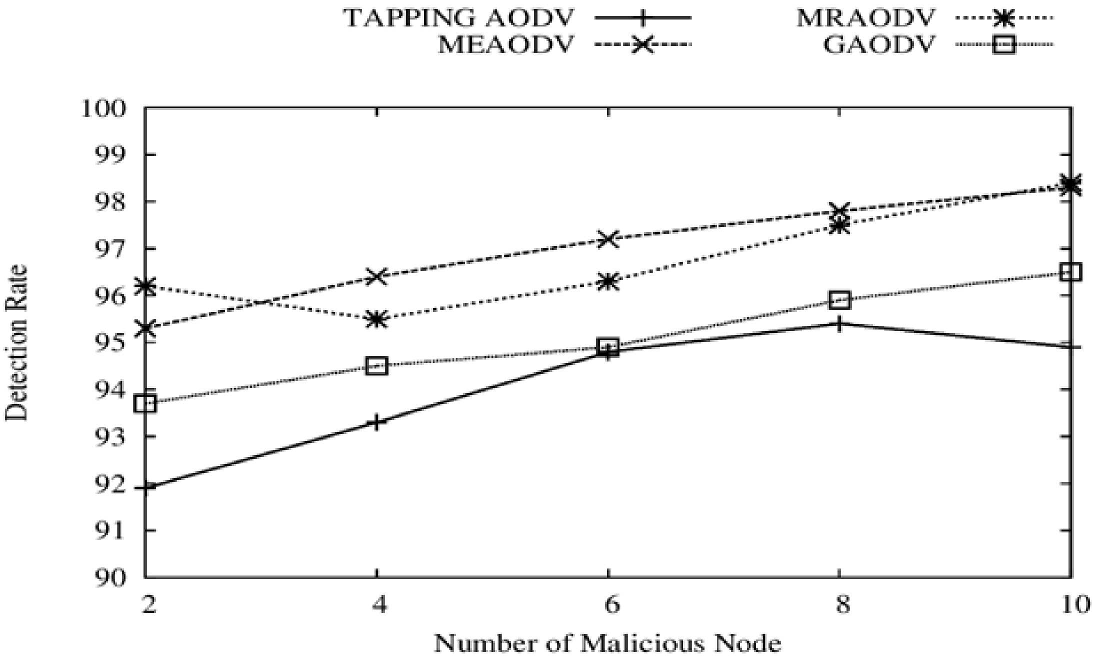

Fig. 4. Detection rate for various detection techniques

Conclusion

As per the simulation outcome performance of AODV is slightly more efficient than the tapping AODV.

IN MRAODV, during route discovery phase MRAODV isolates Black hole and sets up a secure route for the transmission of the data. It also attempts to reduce normalized overhead by decreasing the number of the forward reply packets which have been sent by the adversaries. Simulation result which has been presented in the form of graphs proves that MR-AODV is a reliable solution that gives significant improvement under various parameter and varied traffic states in PDR with moderate average end-to-end delay.

In GAODV, slight modification in the protocol can show that a single run algorithm can detect the presence of Black Hole, also with the modification in their method they have also achieved the success in detection of time varying and target varying black holes. Their simulation result also shows that their algorithm is packet traffic efficient as well as time efficient.

In MEAODV PDR increases comparatively on increasing the number of nodes, but end-to-end delay fluctuates. Here we have concluded that the AODV with MEAODV methods give comparatively better performance.

According to the above study we have concluded that the ME-AODV and MRAODV detection techniques are the best detection technique as they provides the best solution for mitigating black hole attack by controlling the routing update with new condition parameter and removing the redundancy in detecting malicious nodes and varying different parameters.

MRAODV and MEAODV detection techniques have the maximum Average throughput which indicates that these two detection techniques are the best among all when we use these techniques because there is very less packet drop.

MEAODV and MRAODV have the highest Detection rate i.e., they are capable of detecting the maximum attack in the network due to the increase in the black hole attack that the hop count of the neighbor.

Acknowledgement

We would like to express our deep gratitude to JECRC Foundation for encouraging us whenever we needed help.

Author’s Contributions

We have studied various detection techniques that have been proposed by various authors and have taken some of the detection techniques and generated a matrix graph. We have analyzed the various detection techniques in different parameters.

Sunil Kumar Jangir: Survey work, investigated all schemes and equated them, worked on performance matrices and drafted the manuscript.

Naveen Hemrajani: Detailed literature study, comprehensive review for all the detection schemes and figured out matrices performance in the form of diagram and drafted the original manuscript.

Ethics

All writers testify that this material has not been published in whole or in part elsewhere and the manuscript is not currently being considered for publication in another journal.

References

Anishi, G., 2013. Black hole attack mitigation method based on route discovery mechanism in AODV protocol. Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research, (ICR' 13).

Arun, K.K.A., 2016. Worm hole-black hole attack detection and avoidance in Manet with random PTT using FPGA. Proceedings of the International Conference on Communication Systems and Networks (CSN' 16), Thiruvananthapuram, India.

Ayesha, S., K. Sridevi and A.A.K. Mohammed 2015. Preventing black hole attacks in MANETs using secure knowledge algorithm. Proceedings of the International Conference on Signal Processing and Communication Engineering Systems, (CES' 15).

Deng, H., W. Li and D.P. Agrawal, 2002. Routing security in wireless ad-hoc networks. IEEE Commun. Magazine, 40: 70-75. DOI: 10.1109/MCOM.2002.1039859

Hizbullah, K., Nizamuddin, Fahad Khurshid and N.U. Amin 2013. Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash. Proceeding of the 10th IEEE International Conference on Networking, Sensing and Control, Apri. 10-12, IEEE Xplore Press, Evry, France. DOI: 10.1109/ICNSC.2013.6548814

Hoang, L.N. and T.N. Uyen, 2008. A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Netw., 6: 32-46. DOI: 10.1016/j.adhoc.2006.07.005

Hu, Y., D.B. Johnson and A. Perrig, 2002. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications Jun. 20-21, pp: 3-3

Jitendra, S. and G. Vinit, 2014. Clustering of mobile ad hoc networks: An approach for black hole prevention. Proceedings of the International Conference on Issues and Challenges in Intelligent Computing Techniques (ICT' 14), Ghaziabad.

Kamarularifin, A.J., Z. Ahmad and A.M. Jamalul-Lail 2011. Securing routing table update in AODV routing protocol. Proceedings of the IEEE Conference on Open Systems, Sept. 25-28, Langkawi, Malaysia.

Maan, F., Y. Abbas and N. Mazhar, 2011. Vulnerability assessment of AODV and SAODV routing protocols against network routing attacks and performance comparisons. Proceedings of the Wireless Advanced (WiAd), Jun. 20-22, IEEE Xplore Press, London, UK. DOI: 10.1109/WiAd.2011.5983282

Mingyan, L., R.R. Talpade and A. McAuley, 1999. Route Ad hoc multicast routing protocol. Technical Report 99, at the Institute for Systems Research, University of Maryland,

Mistry, N.H., D.C. Jinwala and M.A. Zaveri, 2009. MOSAODV: Solution to secure AODV against Blackhole attack. Int. J. Comput. Network Security.

Mohamed, A.A. and J.B.K. Peter, 2016. Resisting blackhole attacks on MANETs. Proceedings of the 13th IEEE Annual Consumer Communications and Networking Conference, Jan. 9-12, IEEE Xplore Press, Las Vegas. DOI: 10.1109/CCNC.2016.7444935

Neha, S. and S.B. Anand, 2016. Detection as well as removal of black hole and gray hole attack in MANET. Proceedings of the International Conference on Electrical, Electronics and Optimization Techniques (EOT' 16), Chennai, India.

Panagiotis, P. and Z.J. Haas, 2002. Secure routing for mobile ad hoc networks. Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (MSC' 02), San Antonio.

Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb. 25-26, IEEE Xplore Press, New Orleans. DOI: 10.1109/MCSA.1999.749281

Perkins, C.E. and P. Bhagwat, 1994. Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers. Proceedings of the Conference on Communications Architectures, Protocols and Applications, Aug. 31-Sept. 02, London, pp: 234-244. DOI: 10.1145/190809.190336

Radhika, K.V. and K.H. Wandra, 2015. A review: Blackhole attack detection/prevention techniques in manet. Res. HUB Int. Multidisciplinary Res. J.

Ramaswamy, S., H. Fu, M. Sreekantaradhya, J. Dixon and K. Nygard, 2003. Prevention of cooperative black hole attack in wireless ad hoc networks. Proceedings of the International Conference on Wireless Networks, (CWN' 03).

Rathiga, P. and S. Sathappan, 2016. Hybrid detection of Black hole and gray hole attacks in MANET. Proceedings of the International Conference on Computation System and Information Technology for Sustainable Solutions (TSS' 16), Bangalore, India.

Royer, E.M. and C.K. Toh, 1999. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Commun., 6: 46-55. DOI: 10.1109/98.760423

Rutvij, H.J., 2013. MR-AODV: A solution to mitigate blackhole and grayhole attacks in AODV based MANETs. Pro 3rd International Conference on Advanced Computing and Communication Technologies, (CCT' 13).

Sakshi, J. and A. Khuteta, 2015. Detecting and overcoming blackhole attack in mobile Adhoc Network. Proceedings of the International Conference on Green Computing and Internet of Things (CIT' 15), Noida, Delhi.

Sakshi, J., 2014. Review of prevention and detection methods of black hole attack in AODV- based on mobile ad hoc network. Int. J. Information Computation Technol., 4: 381-388.

Sanjay, K.D., I. Woungang, R.M.P. Khurana, 2013. GAODV: A modified AODV against single and collaborative Black Hole attacks in MANETs. Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops, (NAW' 13).

Sanzgiri, K. and B. Dahill, 2002. A secure routing protocol for ad hoc networks. Proceedings of the International Conference on Network Protocols, (CNP' 02), Paris, France.

Sanzgiri, K., B. Dahill, B.N. Levine, C. Shields and E.M. Belding-Royer, 2002. Secure routing protocol for Ad-Hoc networks. Proceeding of the 10th IEEE International Conference on Network Protocols, Nov. 12-15, Santa Barbara, pp: 78-87.

Satoshi, K., H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, 2007. Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. Int. J. Netw. Security, 5: 338-346.

Semih, D., Y.M. Erten and C.E. Acar, 2007. Performance analysis of ad-hoc networks under black hole attacks. IEEE Southeast Conference, Mar. 22-25, IEEE Xplore Press, Richmond, pp: 148-153. DOI: 10.1109/SECON.2007.342872

Shalini, J., 2010. Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. Int. J. Comput. Applic.

Sukla, B., 2008. Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. Proc. World Congress Eng. Comput. Sci.

Tamilselvan, L. and V. Sankaranarayanan, 2007. Prevention of blackhole attack in MANET. Proceedings of the International Conference on Wireless Broadband and Ultra Wideband Communications, Aug. 27-30, Sydney, Australia.

Thi, N.D. and C.K. Yeo, 2016. Detecting colluding blackhole and greyhole attacks in delay tolerant networks. IEEE Trans. Mobile Comput., 15: 1116-1129. DOI: 10.1109/TMC.2015.2456895

Tseng, F.H., L.D. Chou and H.C. Chao, 2011. A survey of black hole attacks in wireless mobile ad hoc networks. Human-Centric Comput. Inf. Sci. Springer Open J.

Vaishali, G.M. and R. Lata, 2015. Security agents for detecting and avoiding cooperative blackhole attacks in MANET. Proceedings of the International Conference on Applied and Theoretical Computing and Communication Technology (CCT' 15), Davangere, India.

Wu, B., J. Chen, J. Wu and M. Cardei, 2007. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. Proceedings of the Wireless Network Security on Signals and Communication Technology, (SCT' 07), Springer, New York. pp: 103-135.

Zhou, L. and Z.J. Haas, 1999. Securing ad hoc networks. J. IEEE Network, 13: 24-30. DOI: 10.1109/65.806983