ISSN: 1304-7981 Number:**9**, Year: **2015**, Pages: **46-57** **http://jnrs.gop.edu.tr**

Gaziosmanpasa University
Graduate School of Natural and Applied Sciences
Journal of New Results in Science

Received: 26.05.2015
Accepted: 16.08.2015

Editors-in-Chief: Bilge Hilal Cadirci
Area Editor: Ahmet Fenercioglu

Black Hole Attacks in Mobile Ad Hoc Networks

Reza Amiri [a] (amirish60@ut.ac.ir)
Marjan Kuchaki Rafsanjani [b,1] (kuchaki@uk.ac.ir)
Ehsan Khosravi [c] (ehsan_k81@yahoo.com)
Hadis Amiri [d] (amirih80@gmail.com)

[a] *ACECR Kerman Branch, Kerman, Iran*
[b] *Department of Computer Science, Faculty of Mathematics and Computer, Shahid Bahonar University of Kerman, Kerman, Iran*
[c] *Department of Computer Science, Sirjan University of Technology, Kerman, Iran*
[d] *ACECR Kerman Branch, Kerman, Iran*

Abstract – Mobile ad hoc networks are used on different occasions, especially during crises. In risk and crisis management, communications is considered vital. With regard to their features, mobile ad hoc networks can be very helpful when dealing with a crisis such as flood, earthquake, war, etc. Security is nowadays considered as one of the main concerns in mobile ad hoc networks. And blac khole attack is among the most important threats of mobile ad hoc networks, where the malicious node places itself along the route by deceiving other nodes and then drops data packets. This paper attempted to investigate a number of proposed solutions against blac khole attacks.

Keywords -
Mobile Ad hoc Networks (MANETs), Risk and crisis management, Intrusion detection, Black hole attack.

1. Introduction

Every single node in mobile ad hoc networks (MANET) is equipped with a transmitter and a receptor, allowing it to communicate with the other nodes within its radio range. To transmit data packets to other nodes outside their radio range, nodes in MANETs require the cooperation of other nodes, referred to as the multi-hop method. As a result, every node can be both a host and a router simultaneously [3].
Mobile ad hoc networks (MANET) are self-organizing networks, which are automatically administered by a collection of mobile nodes without any pre-established infrastructure or centralized administration [16]. As a result of dynamic topology, independence from infrastructures, self-organization, and facility of movement, MANETs are considered a desirable option for military (communication of stations, automated fronts, tactical networks) and non-military crisis management (search and rescue and recovery of catastrophic events) [10]. As defined by IETF a MANET is an autonomous system of mobile nodes connected by wireless links. The network's wireless topology may change rapidly and unpredictably [13].

[1] ***Corresponding Author***

MANETs are extremely vulnerable to malicious attacks, thus security of these networks is considered an important research topic. First, most routing protocols in ad hoc networks lack security measures to protect the routing process. And intruders can easily fake route packets in order to alter the destination or route nodes. Second, free nodes are independent nodes, able to move freely within MANETs; meaning that weakly secured nodes are exposed to abduction, and managing all free nodes are extremely difficult due to dynamic topology . Third, there is no centralized authority (CA) in MANETs. By disconnecting the cooperation mechanism of nodes, using the mentioned weakness, intruders can attack the network. Without authentication, the intruder forges a node to gain unauthorized access to sensitive resources and information and interfere with the performance of other nodes.
MANETs like other wireless networks are vulnerable against active and passive attacks. Passive attacks merely cause eavesdropping of data, while active attacks trigger operations such as repetition, changing, or removing of data. Attacking the network, malicious nodes can cause nodes to overcrowd, spread false routing information, and prevent proper service. Through sending a routing packet to other nodes, malicious nodes claim to have the shortest route to the destination, and so place themselves on the route. Then drop the packets without sending them [11].
Intrusion prevention and intrusion detection are two major security lines in the related literature.
This paper investigates black hole attack and the methods for its detection. The second section addresses black hole attack and its different types. Types and necessity of security systems in MANETs are discussed in section 3. In section 4, a couple of proposed security methods for MANETs are introduced and, in Section 5 we conclude the paper.

1. Black hole Attack

The black hole attack is an attack in network layer which drops all packets by sending fake route replies. The intruder can navigate packets to different destinations to itself and drop them, or otherwise, concentrate all the routes in a network towards a node, while the destination is elsewhere [12].
There are two types of black hole attacks.
In single black hole attacks: a single node compromises the routing process. The black hole attack involves in a malicious node sending a fake routing reply and advertising it to be an optimum route to the destination and makes the other nodes in the network to choose it as the route for their information packets. The malicious node can, then, easily sabotages the system [1].
Cooperative black hole Attack: some malicious nodes cooperate for deceiving the creation and transmission of routing information. In a cooperative black hole attack, malicious nodes work in teams. Consider, for instance figure 1. Here, node S is the source and node D, the destination node, with nodes 1 through 4 acting as intermediate nodes, and nodes 4 and 5 are cooperating black hole nodes.

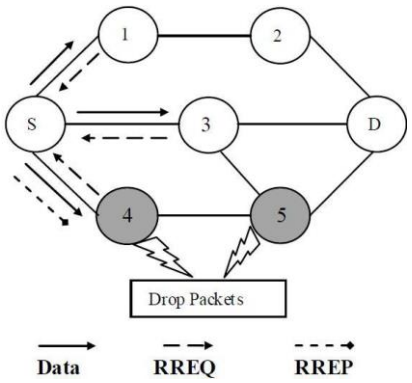

Figure 1: Cooperative black hole Attack [2]

In an attempt to transmit data to the destination, the source node initially sends a Route Request (RREQ) packet to its neighbors; while, instead, black hole nodes immediately send a Route Reply (RREP) packet to the source. The transmitted RREP packet from node 4 reaches the source, and in the meantime, replies from other nodes in the network are also received. Considering the fact that node 4 has proposed the best route, the source chooses this route for data transmission. Instead of transmitting packets to the destination, node 4 forwards them to its cooperating node 5, where the packets are dropped or altered. In such a manner, eavesdropping of node S fails to detect node 4 as an intruder. Meanwhile, nodes 4 and 5 drop data packets and make intrusion detection even harder.

3. Security Protocols for MANETs

3.1. Intrusion Prevention System

One general way to secure the network is using intrusion prevention protocols. This protocol adopts data encryption for identity verification and authentication, as well as, blocking eavesdrop by other nodes [7].
Intrusion prevention method centers on securing the network against intruders by augmenting encryption techniques or employing more secure protocols. However, intrusion prevention methods, alone, are not sufficient for securing MANETs. Preventing internal attacks by malicious users are extremely difficult. Securing a MANET requires the employment of detecting and response techniques as well as matching these techniques to new environments [14].

3.2. Intrusion Detection Systems

In case an intruder manages to bypass the intrusion prevention system, the intrusion detection system will be responsible for detecting the intruder. In other words, intrusion detection systems are considered as a second layer security for a network. Some of the definitions of intrusion detection systems will follow:
[15] Introduces intrusion detection as a complementary mechanism for data protection in all the applications of MANETs.
[4] Maintains that an intrusion detection system is capable of detecting malicious activities or internal attacks posed by the network's compromised nodes, targeting network resources. These systems, then, try and prevent intrusions which threaten network security, and even go further and struggle to repair the damages inflicted by the intruder. Therefore,

subsequent to detecting new vulnerabilities, an intrusion detection system effectively and efficiently detects and neutralizes attacks.
Intrusion detection in [6] is defined as a major part of network security which adds an extra defense layer against misuse, besides physical control, access control, and authentication.
As stated by [1], intrusion detection protocols are considered among the major techniques adopted against security threats. Intrusion detection is the process of detecting an intruder and preventing the consequences of its intrusion.
[8] Defines an intrusion detection system as tools, methods, and resources which assist the process of detection, identification, and reporting of illegal or unauthorized activities.

3.2.1. Different Types of Intrusion Detection Systems Based on Detection Technique

Intrusion detection systems can be divided into three categories based on the intrusion techniques utilized:

- Misuse or signature intrusion detection system: this method contains available and known attack signatures and uses them for intrusion detection by comparing them to the incoming traffic. Expert system, pattern recognition, colored petri-nets, and state transition analysis, are some instances of misuse intrusion detection techniques.
- Anomaly intrusion detection system: the aim and attempt of an anomaly intrusion detection system is to detect activities which lack normal and expected behavior. Techniques such as statistics, neural networks, and other data mining methods are placed within this category of detection methods.
- Specifications-Based Intrusion Detection System: this is a combination of anomaly and signature intrusion detection systems, operating based on a finite - state machine. Besides being capable of detecting unknown attacks, this technique reduces false positives as well. However, this method is limited to the protocols defined.

4. Different Proposed Techniques for Detection of black hole Attacks

4.1. Preventing black hole attack in MANETs using Anomaly Detection

In 2010 an intrusion detection system was proposed entitled 'Preventing black hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection' [1]. This method provides an intrusion detection, which prevents black hole attacks by single and multiple intruders using anomaly detection.
This method assumes that all the activities of the user and system can be monitored and can distinguish abnormal activities of an intruder from normal network behavior, it, then, requires a set of predefined abnormal behavior. Each and every node in this method is responsible for protecting itself against this attack, yet, no warnings is transmitted to another node, that is, this method only uses host-based intrusion detection. In a black hole attack, the intruder deceives the source node by sending a false route reply (RREP) packet. A false route reply packet entails:

- A high destination sequence number: in order for the route to be updated.
- Low hop counter: to make the route seem short and be chosen by the source node.
- Long route life span: to make the route seem as a stable route with a long life span.

The intrusion detection system considers the above information as the attack signature, and in case an RREP packet matches the above description, the system considers the source node as an intruder, therefore waits for another RREP packet for route selection. Simulation results indicate that network has improved, assisted by the proposed method. However, in this method, the intruder can deceive the intrusion detection process by

eavesdropping on the exchanged packets and the guessing destination sequence number and appropriate hop counter. This method also suffers from a high possibility of false positives

4.2. Improving AODV Protocol against Black hole Attacks

[9] Proposed a method titled 'Improving AODV protocol against black hole attacks'. This process is mainly based on analysis and security improvement of AODV protocol.
In original AODV, the source node, by default, accepts the first transmitted RREP packet, whereas, in the proposed method, all the RREPs will be stored in a table called Cmg_RREP_Tab, where, they remain until MOS_WAIT_TIME. The contents of this table are up-dated every time an RREP is selected. Upon receiving the RREP control message, the source node waits as long as MOS_WAIT_TIME, this is when the added function of Pre_ReceiveReply is executed. The source node analyzes all the RREP packets stored on Cmg_RREP_Tab. In case an RREP packet has a higher destination sequence number than the source sequence number, the transmitter suspects the presence of a malicious node. The control messages of the suspicious node are ignored until detection of the intruder. The variable Mali-node is retained to reject all the received control messages from the malicious node. Upon detection, a routing table is no more retained for the malicious node, and its control messages are not forwarded in the network. However, this method will fail when encountered with the cooperative black hole attack. Also, there is a high possibility of false positives.
Comparing the proposed and AODV methods, the packet delivery ratio in node mobility was 70.86 for AODV and 70.87 for the proposed method. However, end-to-end delay had a 6.28% increase.

4.3. Detection and Removal of Cooperative Black/Gray hole Attack in Mobile Ad hoc Networks

[21] Introduced a mechanism called 'detection and removal of cooperative black/gray hole attack in mobile Ad hoc networks'. This solution is capable of identifying cooperative malicious nodes with high packet drop rates.
Following this method, initially, a backbone network (BBN) is developed across the network composed of powerful and reliable nodes. The source node sends a request to one of BBN nodes for a unique and unused IP called Restricted IP (RIP). BBN nodes allocate an RIP to any authenticated node. The source node sends an RREQ to the destination node and the RIP address. If the source node receives only the RREP of the destination node, there is no black hole. Otherwise, if the source receives RREP packet for the RIP, it is possible that there is an intruder in the network. Upon receiving the warning message from the source node, the neighboring nodes shift to irregular state. Neighbors monitor the transmitted packets to and from malicious nodes. In this method, a few faked data are sent by the source node to test the malicious node. The neighboring nodes monitor the packet flow and in case the dropping rate is higher than normal threshold, they regard it as a black hole and inform the source node of the presence of a malicious node. This proposed method is capable of detecting not only black hole, but also the gray hole attack.

4.4. Preventing Black hole Attack in MANETs using Intrusion Detection

The method of prevention of selective blackhole attacks on mobile ad hoc networks through intrusion detection systems, here referred to as PSBA, was introduced in 2011

[19]. Intrusion detection nodes in this method are considered fixed, and after they detect a malicious node, intrusion detection nodes broadcast an alert message throughout the network to inform the other nodes of the presence of a malicious node. The Anti-Black hole Mechanism (ABM) algorithm implemented for intrusion detection nodes are comprised of two Records RREQ (RQ) and Suspicious Node (SN) tables. The RQ table stores PREQ messages observed by the intrusion detection node within its transmission range. SN table is employed for an intrusion detection node to store the degree of suspicion of nodes within its transmission range. The degree of suspicion of a node is crucial for judgments made concerning the malicious node. In case an intermediate node, is not a destination node, and does not transmit an RREQ packet for a certain route, but forwards RREP for the route, then, its degree of suspicion is increased one unit in the SN table of the monitoring intrusion detection node. If the level of suspicion is lower than a threshold value, it will be considered as an inactive status, otherwise, the status is identified as active and the node will be blocked.
Comparison results from the proposed and AODV methods show packet delivery ratio in node mobility at 92.40 for AODV and 10.05 for the proposed method.

4.5. An Application Layer Scheme for Intrusion Detection in MANET Using Mobile Agents

In 2011, a method was proposed for intrusion detection by introducing an application layer scheme for intrusion detection in MANET using the mobile agent of (TraceGray) [20]. Every node monitors only the next node and there is no need for irregular monitoring. Gray hole attack in ad hoc networks can be detected by this method.
When a node detects suspicious behavior, it starts the detection process by creating mobile agents. Consider, for instance figure 2 where D is the destination node and C an intruder. Streams 1, 2, and 3 take place and the mobile agent returns to node A again, then, the algorithm moves one step forward, now node B is considered as the beginning of the algorithm, and the mobile agent moves over to node C. Using the stored route information in the data packet of the next node, node D is detected and the mobile agents move to node D. But since no data packet has reached node D, it cannot transmit the data to the source (node B), therefore, node C is considered an intruder.

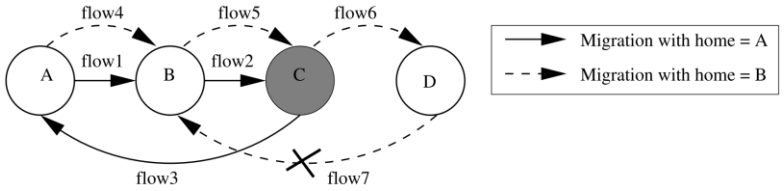

Figure 2: Movement of the mobile agent for intrusion detection (node C is an intruder) [20]

As the proposed method operates based on a mobile agent which detects any gray hole node on the route from source to destination, the number of hops between the source and the gray hole node influence the method's efficiency. Simulation results indicate that the more the number of the hops, the more delayed the detection will be. Furthermore, an increased number of hops lead to a rise in the number of packets required by the mobile agent for detection, and as a result, a higher overload will be imposed on the network.

4.6. Preventing Black hole Attack in DSR based Wireless Ad hoc Networks

This method of preventing black hole attack in DSR based wireless Ad hoc networks was introduced in 2012, which, besides detecting black hole attacks, it identifies the location of black hole nodes [17]. This method detects both single and cooperative black hole attacks. Behavior of suspicious nodes is monitored in both stages of detecting and positioning, and so, application of forged information by malicious nodes is prevented.
In the proposed method, generally, there is a node for every single node with maximum reliability among one hop neighbors, called local most trusted node. An intermediate node producing an RREP is required to send a Trace request (TREQ) to its next-hop nodes towards the destination. The corresponding LMT node and the intermediate node initialize a timer. When the next-hop node receives the TREQ, it sends back a Trace reply (TREP) and forwards the TREQ to its next-hop node. As soon as the TREP message reaches the previous intermediate node, the LMT timer stops. Otherwise, if the previous intermediate node that generated the RREP does not receive the TREP, a timeout occurs, which indicates that RREP is fake and there is a black hole attack. During detection, the corresponding LMT monitors the behavior of intermediate nodes. In addition, in the positioning mechanism, nodes that send faked RREP are traceable. In case an intermediate node fails to receive the TREP from its next-hop node towards the destination, it must send an RERR to the destination. This process is monitored by the corresponding LMT node. Therefore, in case an intermediate node refuses to transmit the RERR message, it can be labeled as a black hole node by the corresponding LMT node.
This proposed method was compared to BDSR, DSR, and CBDS, and the simulation results showed that this method shows a higher efficiency (packet delivery ratio).

4.7. Black hole Combat Using Node Stability System in MANET

The black hole combat using the node stability system in MANET was proposed in 2012[5]. This method employs Node Stability System (NSS) to detect single and cooperative black hole nodes. According to this method, an ID is given to every node intending to enter the network. This ID is only given to network members and is hidden from external nodes or hackers. Security values are allocated to every node, which is broadcast to other nodes in certain intervals so that these nodes can update the values on their security table. Every node in this method creates its own security table, and the participant nodes determine a Network Security Level (NSL), divided into four sections of reply collection, route discovery, NSL updating, and black hole isolation. Stability of each node is shown in NSL, therefore, if the network security level of each node is zero, black hole has occurred, and the node is marked as a malicious node.

4.8. Detecting Black hole Attacks on DSR-based mobile Ad hoc networks

The present study introduces a new method for detecting Black hole Attacks on DSR-based mobile Ad hoc networks referred to as DBA-DSR [22]. As a modified version of DSR protocol, this protocol is capable of detecting and removing black hole nodes before the original routing mechanism begins, through sending faked RREQ packets.
An acknowledgment scheme (ACK) is used here, such that data packets are transmitted only when the source has received the ACK reply. So, if a problem arises in the initial stage of faked route reply packets, the proposed method can detect black hole nodes by sending and receiving ACK packets.

Faked RREQs use fake destination addresses for detecting black hole nodes and only live for a certain period of time. In this method, a field is added to the RREPs of the original DSR to include the addresses to nodes which have started route reply.
The source node first creates an RREQ with a fake address and broadcasts it across the network. Upon receiving this packet, the malicious node produces an RREP, and sends it across to the source node. Having received this reply, the source node notices the existence of malicious activity within the network. Then, by analyzing the RREP, and the identification of the creator, the intruder is identified. The address to this malicious node is then added to the black hole node table. Nodes in this table are excluded from all routing processes. The proposed method was compared to DSR protocol. The results indicated higher packet delivery rate and efficiency of the proposed method with black hole present compared to DSR.
A comparison of intrusion detection systems: the proposed intrusion detection systems that introduced in this section are evaluated and compared in table 1.

4.9. Cross-layer Detection for Black hole Attack in Wireless Networks

The Cross-layer Detection for Black Hole Attack in Wireless Networks was developed to detect black hole and gray hole attacks in ad hoc networks, following a cross-layer design [23]. At the network layer, a route-based method is proposed for eavesdropping on next-hop activities. In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold in order to lower the false positive rate under high network overwork. The above design does not broadcast within the network any extra control packet and preserve network resources for detection nodes. Simulation results on DSR protocols indicate an average detection rate of approximately 90 percent and a false positive rate of 10 percent.
Black hole attack misleads routing protocols by deceiving other nodes concerning routing information. This is a route-based method. A single node cannot manage to observe all the neighboring nodes, and can only see its one-hop neighbors.
One of the problems of this method, is a high probability of false positives during high network traffic (network traffic peak). The cause for the high possibility of false positives is hidden nodes in the protocol of carrier-sensing multiple-access with collision avoidance (CSMA/CA).
To obviate the problem of hidden nodes, a cross-layer mechanism is proposed in this method. The two counters of collisionPktNum and nonColPktNum are incorporated into the standard protocol of 802.11. In case of a collision, collisionPktNum increases one unit, and in case a packet is received successfully, nonColPktNum increases one unit instead. During the fixed time period, collision is calculated as follows:

$$RCR(N) = \frac{collisionPktNum}{collisionPktNum + nonColPktNum}$$

The collision rate is reported to the layer and counters are set to zero. The accumulated collision rate is calculated in the network layer.

4.10. Geographic Routing Used in MANETs for Black hole Detection

Geographic routing used in MANETs for black hole detection employs a modified associativity based routing (MABR) protocol. This routing protocol is based on a Modified Associativity of the Associativity Based Routing (ABR). Intermediate nodes in this protocol, receive RREQs from the source node and via investigating their positioning table, determine if there is a valid route to the destination [18].

MABR uses positioning information of nodes for route discovery. With the assistance of GPS, this information is gathered and sent to the neighboring nodes. In this way, every node is informed of its neighbors.
Every single node in geographic routing, benefits from a positioning table, which plays a major role for positioning all nodes in the MBAR. Characteristic to this table are neighboring nodes and their positions. The neighboring nodes list all nodes in their vicinity and acquire their positions by intrusion detection via global positioning system (GPS). This method assumes that nodes cannot change their positioning information table, which seems rather unrealistic in actuality. Also, intruders can easily change their positioning information table and send it to the source node and by doing so, deceive the source node and commit intrusion.

Table 1: Comparison of intrusion detection systems

Introduced System	**Task Conducted**	**Investigated Attack**	**Advantages**	**Disadvantages**
Preventing black hole attacks in MANETs using anomaly detection [1]	Using sequence and hop number	Single and cooperative black hole	No additional computational overload is imposed on intermediate and destination nodes, ease of implementation	High probability of false positives, probable deception of intrusion detection system by intruders
Improving AODV protocol against black hole attacks [9]	Using source and destination sequence numbers	Black hole	No additional computational overload is imposed on intermediate and destination nodes ease of implementation	Failure against cooperative black hole attacks
Detection and removal of cooperative black/gray hole attack in MANETs [21]	Using RIP for intrusion detection	Single and cooperative black and gray hole	Detection of cooperative attacks with any number of intruders	Method failure if backbone nodes are intruders
PSBA [19]	Using stable intrusion detection nodes	Single and Cooperative black hole attack	No additional computational overload is imposed on regular nodes	Intrusion detection systems are considered stable which contradicts the movability of MANETs and lessens its flexibility
An application layer scheme for intrusion detection in MANETs using mobile agents [20]	Using a mobile agent to prevent gray hole attacks	Gray hole attack	Can be implemented on all routing algorithms can be extended to all layers of the protocol for detecting attacks in other layers	As the mobile agent is a software, intrusion is impossible

Introduced System	Task Conducted	Investigated Attack	Advantages	Disadvantages
Preventing black hole attack in DSR based wireless Ad hoc networks [17]	Intrusion detection by choosing LMT nodes and examining RREPs	Single and cooperative black hole	Selecting lower-speed nodes as LMT node	Imposes load on the network for selecting LMT nodes and fails to recognize the selected black hole
Black hole combat using node stability system in MANET [5]	Calculation of security level for nodes across the network	Single and cooperative black hole	Using the most secure route for sending packets	As selecting the black hole is dependent on the security level to fall to zero, it will fail against selective black hole
Detecting Black hole Attacks on DSR-based MANETs [22]	Intrusion detection by sending faked packets and examining received ACKs	Single and cooperative black hole	Ease of implementation intrusion detection before sending main data packets	Continual sending of faked packets before sending the data imposes overload on the network
Cross-layer Detection for Black Hole Attack in Wireless Networks [23]	Using a cross-layer mechanism and eavesdropping on next-hop nodes	In single black hole attacks	Using dynamic threshold for intrusion detection	Fails against cooperative black hole attacks
Geographic routing used in MANETs for black hole detection [18]	Using positions of neighboring nodes	Single and cooperative black hole	Reduces delay in route discovery	This method postulates that nodes cannot send fake positions to other nodes Using GPS on nodes

5. Conclusion

This paper provided a brief account concerning MANETs, its weak points, black hole attack, and intrusion detection systems. Then, a number of black hole attack detection and prevention methods were analyzed. As indicated by the results, the proposed methods for detection of black hole attacks suffer from major weaknesses, and some carry assumptions which seem unrealistic. It is, for instance, assumed that systems are not able to change their positioning information, whereas, a compromising system can send faked positioning information by changing software and hardware. Concerning the shortcomings mentioned herein, it is concluded that black hole attack is still considered as a major threat in MANETs and no absolutely proper solution has been yet proposed for preserving the network against this attack.

References

[1] Y.F. Alem and Z.C. Xuan, Preventing Black Hole Attack in Mobile Ad-Hoc Networks Using Anomaly Detection, Proceedings of the International Conference on Future Computer and Communication (ICFCC), 2010, Volume: 3, pp: 672-676.

[2] S. Banerjee and K. Majumder, A Survey of Black Hole Attacks and Countermeasures in Wireless Mobile Ad-Hoc Networks, Proceedings of the International Conference on Recent Trends in Computer Networks and Distributed Systems Security Communications in Computer and Information Science, 2012, Volume: 335, pp: 396-407.

[3] J. Ben Othman and L. Mokdad, Enhancing Data Security in Ad Hoc Networks based on Multipath Routing, Journal of Parallel and Distributed Computing 70 (2010) 309-316.

[4] K. Chang and K.G. Shin, Application-Layer Intrusion Detection in MANETs, Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS), 2010, pp:1-10.

[5] R. Chatterjee and M. Routray, Black Hole Combat Using Node Stability System in MANET, Signal Processing and Information Technology (2012) 249-254.

[6] A. Esfandi, Efficient Anomaly Intrusion Detection System in Adhoc Networks by Mobile Agents, Proceedings of the 3rd International Conference on Computer Science and Information Technology (ICCSIT), IEEE 2010, Volume: 7, PP: 73-77.

[7] N. Jaisankar, R. Saravanan and K.D. Swamy, A Novel Security Approach for Detecting Black Hole Attack in MANET, Information Processing and Management, (2010) 217-223.

[8] R. Mahapatra, N. Garg, R. Sharma and P. Pal, Interaction Between Nodes in MANET, Proceedings of the International Conference on Computational Intelligence and Computing Research (ICCIC), IEEE 2010, pp: 1-5.

[9] N. Mistry, D.C. Jinwala and M. Zaveri, Improving AODV Protocol Against Blackhole Attacks, Proceedings of the International Multi Conference of Engineers and Computer Scientists, 2010 Volume 2.

[10] P. Moradiya and S. Sampalli, Detection and Prevention of Routing Intrusions in Mobile Ad Hoc Networks, Proceedings of the International Conference on Embedded and Ubiquitous Computing, IEEE/IFIP 2010, pp: 542-547.

[11] M. Kuchaki Rafsanjani, A.A. Khavasi and A. Movaghar, An efficient method for identifying IDS agent nodes by discovering compromised nodes in MANET, Proceedings of the Second International Conference on Computer and Electrical Engineering ICCEE'09, 2009, Volume:1, pp: 625-629.

[12] R. Raja Mahmood and A. Khan, A Survey on Detecting Black Hole Attack in AODV-Based Mobile Ad Hoc Networks, Proceedings of the International Symposium on High Capacity Optical Networks and Enabling Technologies, 2007, pp: 1-6.

[13] S.A. Razak, S. Furnell, N.L. Clarke and P.J. Brooke, Friend-assisted Intrusion Detection and Response Mechanisms for Mobile Ad Hoc Networks, Ad Hoc Networks 6 (2008) 1151-1167.

[14] M.A. Ritonga and M. Nakayama, Manager-Based Architecture in Ad Hoc Network Intrusion Detection System for Fast Detection Time, Proceedings of the International Symposium on Applications and the Internet SAINT, 2008, pp: 76-82.

[15] M. Sayee Kumar, S. Selvarajan and S. Balu, ANODR Based Anomaly Detection for Black Hole and Route Disrupt Attacks, Proceedings of the International Conference on Computing, Communication and Networking, IEEE 2008, pp: 1-5.

[16] S. Schuhmann and L. Volker, Combining Passive Autoconfiguration and Anomaly-Based Intrusion Detection in Ad Hoc Networks, Proceedings of the Eighth International Workshop on Applications and Services in Wireless Networks, IEEE 2008, pp: 87-95.

[17] F. Shi, W. Liu and D. Jin, Preventing Black hole Attack in DSR-Based Wireless Ad Hoc Networks, Computer Science and its Applications (2012) 953-969.

[18] M. Shobana, R. Saranyadevi and S. Karthik, Geographic Routing Used in MANET for Black Hole Detection, Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, 2012, pp: 201-204.

[19] M.Y. Su, Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems, Computer Communications 34 (2011) 107-117.

[20] A. Taggu, TraceGray: An Application-layer Scheme for Intrusion Detection in MANET Using Mobile Agents, Proceedings of the Third International Conference on Communication Systems and Networks (COMSNETS), 2011, pp: 1-4.

[21] K. Vishnu and A.J. Paul, Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile AdHoc Networks, International Journal of Computer Applications 1(2010) 40-44.

[22] I. Woungang, S. Dhurandher, R. Peddi and M. Obaidat, Detecting Black Hole Attacks on DSR-based Mobile Ad Hoc Networks, Proceedings of the International Conference on Computer, Information and Telecommunication Systems (CITS), 2012, pp: 1-5.

[23] P. Yi, T. Zhu, N. Liu, Y. Wu and J. Li, Cross-layer Detection for Black Hole Attack in Wireless Network, Journal of Computational Information Systems 8 (2012) 4101-4109.