Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 5; July-September, 2016, pp. 396-400
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

# Detection of Black and Gray Hole Attack in Manet: A Review

**Benzeer Kaur[1] and Harleen Kaur[2]**

[1]*Department of Computer Science & Engineering, Baba Farid College of Engineering and Technology, Deon, Bathinda, India*
[2]*Department of Information Technology & Engineering, Baba Farid College of Engineering and Technology, Deon, Bathinda, India*

**Abstract—***A mobile ad-hoc network (MANET) is a wireless mobile communication. It is a temporary network. It is setup by the group of multi-hop and self-conFig. d mobile nodes. MANET is without any network infrastructure or access points. Mobile unique characteristics such as dynamic topology, infrastructure less, node mobility, self-conFig. d and self-organizing makes it different from other networks but these types of networks are more prone to various types of attacks. In mobile ad-hoc network, any node leaves or joins the network any time. The mobility and dynamic nature of node in the network, the malicious node easily enters in the MANET. The malicious node through various types of attacks easily enter in the network like gray hole attack, black hole attack, routing attack, message altering attack etc. The Black hole and Gray hole packet dropping attack, easily enter in the network through a malicious node. Due to these attacks in the network there is an impact on the different network performance metrics such as throughput, packet delivery ratio and normalized routing load etc. Protecting the network layer from attacks is an important and challenging security issue in mobile ad-hoc networks (MANET) .*

**Keywords**: *Mobile ad hoc networks, black hole, gray hole, detection method*

## 1. INTRODUCTION

A Mobile Ad Hoc Network is a set of mobile nodes that forward packets for each other [10]. MANETs have some special characteristic features such as unreliable wireless links, limited bandwidth, battery power, low computation power etc. Mobile network exchange information without any access point . Mobile ad-hoc network is a temporary network.

**Fig. 1: Mobile ad-hoc network [16]**

MANETs are vulnerable to various types of attacks like warm hole, rushing attack, impersonation, eavesdropping, and denial of service attack etc. Mobile ad-hoc network is a temporary network and nodes are always in moving state [18] .The various application of mobile ad-hoc network like tactical network, emergency service, education, home enterprise etc. MANET is Multi-hop wireless network [3]. Routing attacks do not disrupt the routing protocol Instead, they cause the data packets. For example, the attacker drops the packets, modify the data and content of the packets, or duplicate the packets it has already forwarded [7]. Another type of packet forwarding attack is the denial-of-service (DoS) attack.

## 2. MANET SECURITY AND ATTACKS

A. Flooding Attack: The flooding Attack is a denial-of-service attack. The malicious node sends the fake packets in the network and disturbs the normal functioning of the network. Nodes under the flooding attacks are unable to receive or forward any packet and all the packets directed to them will be discarded from network[13]

B. Impersonation: A node may disguise as another node and send fake routing information to some other normal node. A malicious node might gain perceptive information and even provide fake information to other nodes [12].

C. Packet Modifying: The intermediate node changes the contents of packets during transmission. In a message modification attack, some changes are made in the routing messages by the attacker. In Ad-HOC Network nodes are free to move and self-organize, relationships among nodes at some times nodes may include the malicious nodes. These malicious nodes might disturb the random relationships in the network to participate in the packet forwarding process, and launch the message modification attacks [13].

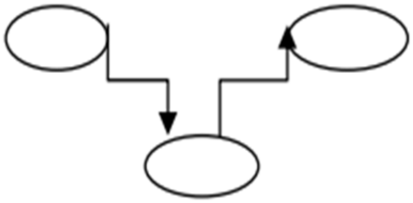

**Fig. 2: Modification [16]**

D. Worm Hole Attack: A worm hole assail is when two or more suspicious nodes work together to encapsulate and exchange messages between them. A worm hole attack always tunnels the packet to its misbehaving partner node [12]. In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network. Routing can be disrupted when routing control message are tunnels. This tunnel between two colluding attacks is known as a wormhole attack.

E. Sink Hole Attack: In sinkhole Attack, malicious node collect wrong routing information to produce itself as a specific node and receives all network traffic. Gray hole attack and black hole attack are most popular examples of sink hole attack [15].

F. Black hole Attack: It is a kind of selfish node that just drops the packets and hence the transmission further. Black hole attack occur on network layer .Black hole gray hole example of sink hole attack. Black hole is a active type of attack. The black hole attack not send any packet to the destination it drops the all packet. In black hole attack not any packet send at destination side, black hole node drop all received packets.[15]

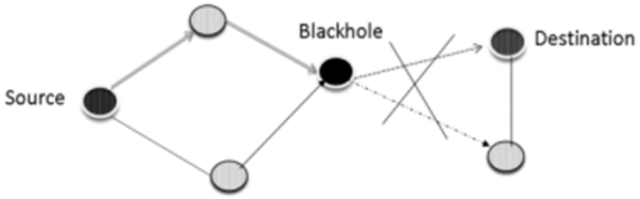

**Fig. 3: Black hole attack [4]**

In Black hole attack, adversary node with help of one of reactive routing protocol announces that it has a valid Shortest route, and once the route is established it drop packets without forwarding to next node.[20]

- Internal black hole attack -In internal black hole attack, malicious node which fits in between the routes of given source and destination and drop all packet.
- External black hole attack- External attacks occur outside of the network and try to access network traffic or disrupting the process of entire network.

G. Gray Hole Attack: The [17] Gray hole attack is also a kind of Denial of service attack. Gray hole attacks is an active type of attack. Gray Hole attack may occur due to a malicious node. A Gray hole attack is a variation of the black hole attack, initially the malicious node is not malicious, it turns malicious sometime later. This attack is more difficult to detect than black hole attack. The malicious node just drop part of the packet not drop all packet. This is called a Gray hole attack. Gray hole attack is harder to find because of some packets reached the destination and destination thinks that it is getting the full data. But the malicious node drop some packet and some packet reach at destination. This is called a gray hole attack.[22]

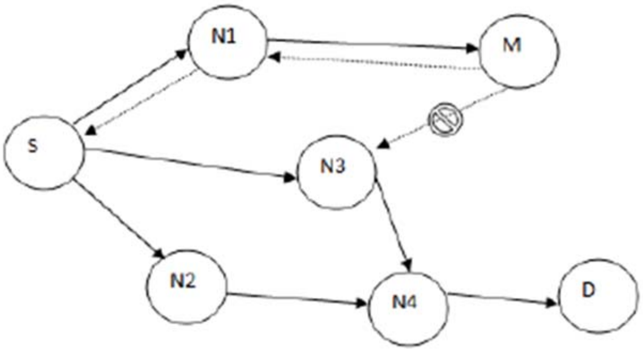

**Fig. 4: Example of Gray Hole Attack [22]**

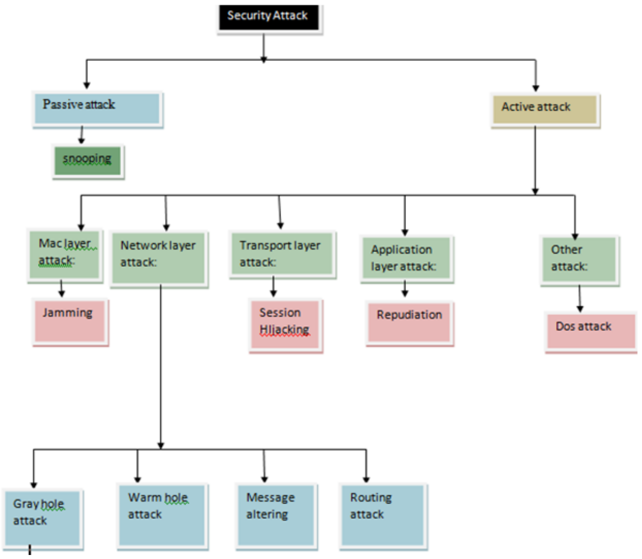

**Fig. 5 Security at different layer [14]**

## 3. LITERATURE SURVEY

**Jaydip Sen *et al.*** Proposed a various security mechanism is to defend against a cooperative gray hole attack on the well known AODV routing protocol in MANETs. The various security mechanisms is proposed to detect these attack. The various mechanisms are used provide security in MANET through: Neighborhood data collection, Local anomaly detection, Cooperative anomaly detection, Global alarm raiser. Simulation results show that the scheme has a significantly high detection rate with moderate network traffic overhead.

**Adnan Nadeem et al**. Proposed Generalized Intrusion Detection & Prevention mechanism .GIDP uses a combination of anomaly and knowledge-based that can protect MANETs against a variety type of attacks like black hole attack, rushing attack and gray hole attack. Simulation results show our proposed mechanism can secure MANETs from a wide variety of attacks with an affordable processing overhead.

**Kimaya sanzgiri et al.** proposed ARAN (authenticated routing for ad-hoc network) and detect various type of attack. ARAN used cryptographic certificate and detect various types of attack. Node used to certificate and after exchange a message. ARAN accepts only those packets that have been signed with certified key. ARAN not accepts these packets that not signed with certified key issue. ARAN provides authentication and non repudiation service. Higher overall routing load and cost of higher latency because the cryptography computation that must occur in network.

**Panagiotis et al.** proposed a SRP (secure routing protocol).The secure routing protocol used a secret association b/w the source and destination and protect the source routing message from various threats. Secure routing protocol collects correct information in timely manner .The protocol define many new feature like query verifiably at destination side. Two nodes securely communicate through a shared secret key in a secure routing protocol.

**YIH-CHUN HU et al.** proposed a Ariadne protocol, which used a TESLA one way key chains and source routing destination pair wise key .The pair wise key to protect the DSR protocol. Ariadne can protect routing message using three scheme.1.Shared secret key used b/w all pair of the node.2.Shared secret key used b/w communicating node combined with broadcast authentication.3.Used digital signature .TESLA is an efficient technique and add only single message authentication code to message for broadcast authentication.

**Aniruddha Bhattacharyya et al.** proposed a various method to mitigate that attack. The various attack identify in this paper like Sybil attack, rushing attack, black hole, gray hole attack etc. The mainly in this paper identify data traffic, and control traffic attack and various method is used to mitigate these attack

**Mohd Faisal et al.** In this paper identify various attacks. In this paper identify various internal and external attacks and identify various active and passive attacks. In future, several security solutions that have been proposed and secure routing protocols will be investigated and classified.

**Meenakshi Patel et al**. Proposed novel automatic security mechanism to detect black and gray hole attack. The SVM is used to defense against malicious attack occurring in AODV.SVM classifies the behavior of the nodes.SVM based system uses PDER, PMOR and PMISR metrics and classifies the nature of nodes. Novel security scheme to detect malicious attack in the MANET .This scheme uses the concept of classification done by SVM. The behavior metrics are used to develop the security system those are easily computed and classify.

**Hizbullah Khattak, et al.** In this paper, a hybrid solution for preventing black and gray hole attack in MANET has been presented. The proposed solution consists of two parts: 1.secure route selection and 2.consistent data transmission. In this paper, hybrid approach for preventing black and gray hole attacks by selecting second shortest route for secure route selection and hash function and timestamp base solution used for consisting data transmission. Hash based solution is used in MANET and message digest scheme is used in source and destination communication message.

**Nisha Puri et al.** In this paper we study the effects of two types of DoS attacks namely like 1.Gray hole attack 2.Black hole attack. The gray hole attack and black hole attack in the network impact on the different performance metrics of the network such as packet delivery ratio and normalized routing load, throughput.

**Usha G et al.** Due to lack of infrastructure support each nodes can and leave join the network at any time. Providing security to these networks is a challenging issue because these types of networks suffer from various type of malicious attacks. One of the attacks which are most difficult to detect in Mobile ad-hoc network is Gray hole attack. In this paper an analytical Gray Hole attack model is developed for AODV protocol. And through analytical model the impact of these attacks easily understood.

**Adnan Nadeem et al** .In this paper proposed a intrusion detection and adaptive mechanism for MANETs that detects a various type of attacks and provides an effective response with low network degradation. In MANET occur various type of attack like black hole, sleep deprivation attack, rushing attack, gray hole attack etc The flexible approach is used to management of threats and improved network performance and low network overhead.

**John Felix Charles Joseph.** Proposed Cross layer based adaptive real-time routing attack detection system for MANETS. Routing detection system that adapt the network changing condition. The efficient methodology for adapting the intrusion detection model at real time. CARRADS use SVM algorithm for detection process in MANET.

**Jan von Mulert et al.** proposed a various security extension. The various security extension of AODV is used in this paper like (SAODV, ARAN etc) and various type of scheme is used to detect various type of attack. The incentive and directional antennae scheme remove various types of threats. The warm hole, black hole, rushing attack ,gray hole attack is detect through these all schemes in this paper and improve network performance..

**Hui Xia et al.** In this paper, MANETs are subjected to a variety of attacks by malicious nodes. The reduce hazards from nodes and enhance the security of network in this paper .Trust prediction model to evaluate the trustworthiness of nodes, which is based on fuzzy logic rules prediction method and the nodes historical behaviors. This method is used to detect a various type of threat.

## 4. TEHNIQUE USED DETECTION OF VARIOUS ATTACKS

- **Detection of malicious node using behavioral approach:** Support vector machine is used to classify the behavior of the node. The detecting behavior or SVM based system used PDER, PMOR, and PMISR and classifies the nature of nodes with the help of SVM classifier [12].
- **Packet leashes:** A packet leash is a technique to prevent wormholes [9] .These may be temporal or geographic. A geographic packet leash requires nodes to know their own location, and contain this information i.e. protected cryptographically into packets. This allows the distance from sender to receiver to be established. Tightly synchronized clocks are required in temporal packet leashes. The packet creation time is included with the packet (encrypted).
- **Directional antennas:** The directional antennas and packet leashes technique used to detect a warm hole attack [9]. Nodes are oriented with several directional zones of transmission, and the direction of transmission is included in neighbor discovery packets. When receiving transmissions, the directional antennas allow a node to establish the range area from which a transmission is received.
- **Generalized intrusion detection and prevention**: Generalized intrusion detection [1] and prevention mechanism used a combination of anomaly based and knowledge-based intrusion detection. Anomaly based technique chi-square test apply on NCM and knowledge based technique apply a rule based approach on NCM and DM and detect a various type of attack like black hole, gray hole, sleep deprivation etc.

## 5. CONCLUSION AND FUTURE WORK

Mobile ad-hoc network has been active research based area over the past few years their application in military and civilian communication. But it is vulnerable to various types of attacks. Misbehavior of nodes causes the damage to the nodes & packet also. The various attacks cause damage to the network & also it is difficult to detect. The performance of the network decreases .In the various researches the intrusions detection & prevention technique, packet leashes techniques are used to detect the attacks in network. This technique is well efficient in improving the performance metrics of the various ADHOC networks. Above mentioned techniques are effective for high detection rate and very low false positive rate and control overhead.

## REFERENCES

[1] Adnan Nadeem, Michael Howarth,"A Generalized Intrusion Detection & Prevention Mechanism for Securing MANETs" 9781-4244-3941-6/09, IEEE,2009

[2] Adnan Nadeem, Michael P. Howarth "An intrusion detection & adaptive response mechanism for MANETs", 368–380, Elsevier, 13 (2014)

[3] Ashok M.Kanthe , Dina Simunic, and Ramjee Prasad., "Effects of Malicious Attacks in Mobile Ad–hoc Networks"International Conference on Computational Intelligence and Computing Research, 978-1-4673-1344-5,IEEE,2012

[4] Aniruddha Bhattacharyya, Arnab Banerjee,dipayan bose "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques" Department of Computer Science & Engineering, Institute Of Engineering & Management, Saltlake

[5] Hizbullah Khattak, Nizamuddin "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET"978-1-4799-0615-4, IEEE, 2013

[6] Hui Xia, Zhiping Jia et al., "impact of trust model on on-demand multi-path routing in mobile ad hoc networks"[ Elsevier, 2012

[7] Haoyang, Haiyunluo,Fanye,Songwulu, Andlixia, zhang "Security in mobile ad-hoc network: challenges and solutions" 1536-1284 ,IEEE,2004

[8] John Felix Charles Joseph, Amitabha Das "Cross layer based adaptive real-time routing attack detection system for MANETS" Elsevier ,2009

[9] Jan von Mulert, Ian Welch , Winston K.G. Seah.,"Security threats and solutions in MANETs: A case study using AODV and SAODV"., Journal of Network and Computer Applications, 1249–1259,Elsevier,2012

[10] Jaydip Sen, M. Girish Chandra, Harihara S.G , Harish Reddy, P. Balamuralidhar" A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks" 1-4244-0983-7,IEEE,2007

[11] KimayaSanzgiri Bridget DahillBrian,Neil Levine, Clay Shields, Elizabeth M. Belding-Royer., "A Secure Routing Protocol for Ad Hoc Networks", Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), 1092-1648, IEEE, 2002

[12] Meenakshi Patel ,Sanjay sharmal., "Detection of Malicious Attack in MANET A Behavioral Approach" 978-1-4673-4529-3,IEEE,2012

[13] Mohd Faisal, M. Kumar, Ahsan Ahmed "ATTACKS IN MANET" IJRET: International Journal of Research in Engineering and Technology Volume: 02, Issue: 10, Oct-2013

[14] Nirali Mod ,Vinit Kumar Guptai et al ., "A Survey Paper On Detection Of Gray-Hole Attack in MANET"[ International Journal of Computer Science & Communication Networks, Vol 4(1), 2012

[15] Nisha Puri, Simranjit Kaur ,Sandeep Kumar Arora., "Performance Analysis of Mobile Ad Hoc Network in the Presence of Sink Hole attack"(IJSER)Volume 1 Issue 3, November 2013

[16] Onkar V. Chandure,Prof. V. T. Gaikwad., "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV

routing protocol in MANET" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011

[17] Onkar V. Chandure, Aditya P. Bakshi , Saudamini P. Tidke , Priyanka M. Lokhande " Simulation of secure aodv in gray hole attack for mobile ad hoc network" International Journal of Advances in Engineering & Technology, Vol. 5, Nov. 2012

[18] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks."In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 27-31, 2002

[19] Saleh Ali K.Al-Omari , Putra Sumari "An overview of mobile ad hoc network for the existing protocol and application" International journal on application of graph theory in wireless adhoc network and sensor network vol.2,no.1 ,march 2010

[20] S.V . Vasantha,DR.A.Damodaram, "Bulwark AODV against black hole and gray hole attack in MANET." 2015 IEEE International Conference on Computational Intelligence and Computing Research 978-1-4799-7849 ,IEEE ,2015

[21] Usha g ,Bose s "An Analytical Approach To Analyze The Impact Of Gray Hole Attacks In MANET" Proc. of Int. Conf. on Advances in Communication, Network, and Computing, DOI: 03.LSCS.1.532,2013

[22] Vani A. Hiremani, Manisha Madhukar Jadhao "Eliminating Co-operative Black hole and Gray hole Attacks Using Modified EDRI Table in MANET", International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), pp. 944-948, 2013

[23] Yih-chun ,adrian perrig , david johnson., " Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks" Wireless Networks Business Media, Inc. Manufactured in The Netherlands, 11, 21–38, Springer Science ,2005