ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY ON WORMHOLE DETECTION AND PREVENTION APPROACH

Malvika Rajput[*], Asst. Prof. C.P. Singh
Computer Science & Engineering Department, Dr. A.P.J Abdul Kalam Technical University
Lucknow, Uttar Pradesh, India

DOI: 10.5281/zenodo.839167

ABSTRACT

Mobile ad hoc network is a dynamic network technology. The topology of network is fully dynamic additionally the centralized control is absent. Since, the network attackers are always trying to break the routing strategy and deploy the attacks. Therefore, the routing protocols are in key role. Among a few different kinds of attack in ad hoc network this paper considers the wormhole attack for investigation. This paper reviews the different techniques utilized for identification of wormhole attack and also suggest a new methodology for avoiding the wormhole attack links.

KEYWORDS: Mobile ad hoc network, Wormhole link, Attack deployment, an avoidance technique.

I. INTRODUCTION

Mobile ad hoc network (MANET) is a type of ad hoc network, which is infrastructure less network. Mobile ad hoc network consists of a collection of wireless mobile nodes that can communicate with each other. These nodes include a laptop, computers, PDAs and wireless phones etc., have a limited transmission range. Such a wireless ad-hoc network is infrastructure less, self-organizing, adaptive and does not require any centralized administration. If two such devices are located within transmission range of each other, they can communicate directly, nodes that are outside each other's range must rely on some other nodes to transmit messages [1]. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host before they reach the final destination. Each node functions as a router. The success of communication highly depends on the cooperation of other nodes.

Since the transmission between sender and receiver may use several nodes as intermediate nodes, many routing protocols have been proposed for the MANETS. Most of Protocol assumes that other nodes are trustable so they do not consider the security and attack issues. The lack of infrastructure, rapid deployment practices, and the hostile environments in which MANETS are deployed make them vulnerable to a wide range of security attacks that are presented in [2], [3], [4].

A. Mobile Ad-hoc network routing protocol

There are different criteria for designing and classifying routing protocols for wireless ad hoc networks. For example, what routing information is exchanged; when and how the routing information is exchanged, when and how routes are computed etc.

a. Proactive (table-driven) routing protocols

These routing protocols are similar to and come as a natural extension of those for the wired networks. In proactive routing, each node has one or more tables that contain the latest information about the routes to any node in the network [5]. Each row has the next hop for reaching a node/subnet and the cost of this route. Various table-driven protocols differ in the way the information about a change in topology is propagated through all nodes in the network. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain a different number of tables. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth. Examples of such schemes are the conventional routing schemes, destination sequenced distance vector (DSDV).

b. Reactive (on-demand) protocols

Reactive routing is also known as on-demand routing protocol since they don't maintain routing information or routing activity at the network nodes if there is no communication [5]. These protocols take a lazy approach to routing. They do not maintain or constantly update their route tables with the latest route topology. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the dynamic source routing (DSR), ad hoc on-demand distance vector routing (AODV).

II. Attacks in Ad-hoc networking

This section provides the information about the various kinds of attacks which are frequently deployed on MANET.

A. Types of attack

There are two main classes of MANET attacks:

a. Active Attack

An active attack, the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network [6]. Active attacks can be an internal or an external attack. The active attacks are meant to destroy the performance of the network in such case the active attack act as an internal node in the network. Being an active part of the network, it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. This attack brings the attacker in a strong position where an attacker can modify, fabricate and replays the messages.

b. Passive Attack

Attackers in passive attacks do not disrupt the normal operations of the network [6]. In Passive attack, the attacker listens to network in order to get information what is going on in the network. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

B. Denial of service attack

The flooding attack is easy to implement but causes the most damage. This kind of attack can be achieved either by using RREQ or Data flooding [7]. In RREQ flooding the attack floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such IP addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding, the attacker gets into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time.

C. Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself as having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way, attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [8]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of a reply from the actual node; hence a malicious and forged route is created. When this route is established, now it’s up to the node whether to drop all the packets or forward it to the unknown address [9]

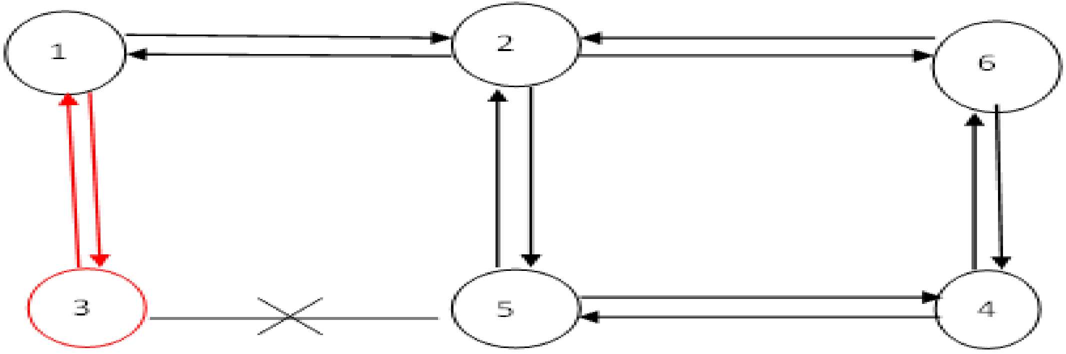

Figure 2 Black-hole attack

The method how malicious node fits in the data routes varies. Fig.2 shows how black hole problem arises, here node ―1 wants to send data packets to node ―4 and initiate the route discovery process. So if node ―3 is a malicious node then it will claim that it has an active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node ―1 before any other node. In this way node ―1 will think that this is the active route and thus active route discovery is complete. Node ―1 will ignore all other replies and will start sending data packets to node ―3. In this way, all the data packet will be lost consumed or lost.

D. Gray Hole Attack

In this kind of attack, the attacker misleads the network by agreeing to forward the packets in the network. As soon as it receives the packets from the neighboring node, the attacker drops the packets. This is a type of active attack. In the beginning, the attacker nodes behave normally and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets, it starts dropping the packets and launch Denial of Service (DoS) attack. The malicious behavior of Gray hole attack is different in different ways. It drops packets while forwarding them in the network. In some other Gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [7]. Due to this behavior, it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack [7].

E. Wormhole Attack

A wormhole is a type of DoS attack. In this type of attack, an attacker obtains the packet from source or neighbor node and transfers it to other malicious nodes (another attacker). Wormhole attack is a tunneling attack in which 2 or more colluding nodes participate. One malicious node sends route packet to another malicious node through a secret channel.

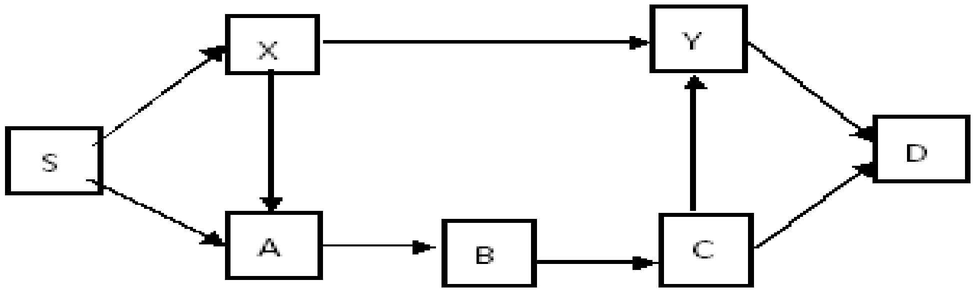

Figure 3 Wormhole attack

Various types of malicious activities are carried out in this secret channel like sniffing, drop, selective-drop of data packets etc.

Worm Hole attack consists of two nodes the attacker nodes that are connected to each other with a link basically this link is known as a tunnel. The attacker node present in the network at one side captures the packet from the legitimate node and encapsulates the packet and with the help of tunnel transmits it to the other attacker node or malicious node present in the network. It consists of one or two malicious nodes and a tunnel between them.

Wormhole nodes fake a route that is shorter than the original one within the network means it create an illusion for the legitimate node so they believe that the route is shorter than the original one. But it is not necessary that the route through wormhole nodes may be shorter. In Figure 4, here we have two malicious node X and Y connected with each other with the help of a link, the link can be wired or wireless, the link is referred as a tunnel, ―the wormhole tunnel‖ through which attacker nodes communicate with each other and all traffic pass through this tunnel. The tunnel can be formed via in-band channel or by out of band channel or through high transmission power. In the Fig. 4, node 5 and node 2 are represented as source and destination respectively. So now the source node 5 will forward the packet to the legitimate neighbor i.e.; node 1in this way intermediate nodes between node 5 and node 2 i.e., 1, 9, 8, 6 will forward the packet from source to destination. In the absence of malicious nodes, the legitimate path from node 5 to node 2 will be 5-1-9-8-6-2 so number of hops the packet travels is 4(four).

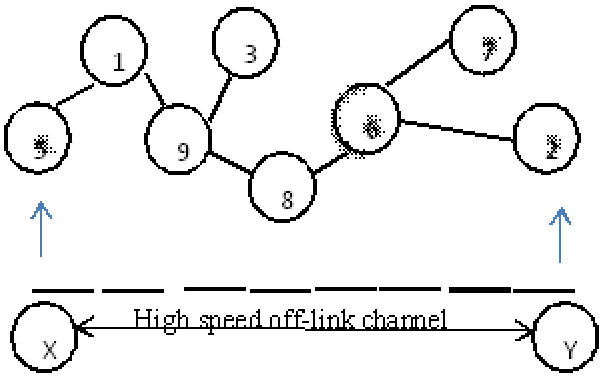

Figure 4 Example of Wormhole Attack

Now when wormhole nodes are present as well as they are malicious nodes so now the nodes X and Y will get activated and these nodes create an illusion to source and destination that they are immediate neighbors and they can hear each other request so transmission takes place between node 5 and node 2 via node X and node Y.

a. Types of Wormhole Modes

The wormhole attack can be launched by given below modes they are listed below as;

I) **Packet Encapsulation or In-band Channel:** In this type of mode the malicious node captures the packet from a legitimate node or source node and encapsulates the packet header of the original packet and designates it to the other malicious node. After receiving the encapsulated packet the other malicious nodes either drop the packet or forward the packet to other nodes which are present in the network. The attacker nodes are within the network.

II) **Out-of Band Channel:** In this type of mode the malicious nodes are connected to each other via an outer link. A channel with high bandwidth is placed between the nodes at the two ends so as they can create wormhole link.

III) **High Power Transmission:** In this type of mode when the source node forwards the packet the attacker node captures it and transmit it to the destination node with a high power, it enforces the nodes to follow the path (the wormhole link) and so that all traffic passes through this link.

Here discussing the type of attacks on their visibility bases. So, they are classified as:

I) **Open Wormhole Attack:** Open wormhole attack is also known as exposed attack; in this type of attack the malicious node include their identity in the packet header. Whenever a node wants to forward the packet it updates its packet header and encapsulate its identity the nodes follow the route discovery procedure. When the malicious node captures the packet, it includes its identity in the packet header as the other authentic nodes do. Hence the legitimate nodes are aware of the presence of the wormhole nodes, these wormhole nodes may not necessarily be malicious. Here both the malicious nodes are visible.

II) **II). Close Wormhole Attack:** Closed Wormhole Attack also known as hidden attack, this of attack does not update the packet header at the time of route discovery process hence the legitimate nodes are unaware of their presence. These nodes capture the packet and transmit the encapsulated packet to the other malicious node with the help of tunnel. After receiving the packet, the other malicious nodes either forward the packet or discard the packet. Here other the malicious nodes are invisible.

III) **Half Open Wormhole Attack:** In this type of attack the malicious node at one side of the network update its identity in the packet header at the time of route discovery process. Here one malicious node is visible and other is invisible to the legitimate nodes in the network.

b. Properties of wormhole attack

MANETs are a new paradigm of networks, offering unrestricted mobility without any underlying infrastructure such as base station or access point. Basically, ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. Following are the characteristics of a MANET [18, 19]:

- Autonomous Terminal
- Infrastructure- less and Self Operated
- Distributed operation
- Dynamic network topologies
- Multi-hop routing

- Energy constrained Operation
- Light –weight Terminal
- Ease of deployment
- Speed of deployment

The detection and prevention of wormhole attack for MANETs are very well investigated and here a summary of the literature is provided, in order to help the reader with a better understanding of the current state of the art. Following each review, we will discuss each of the proposed methods on their applicability to MANET.

III. RELATED WORK

A transmission time-based mechanism (TTM) to detect wormhole attacks – one of the most popular & serious attacks in Wireless Ad Hoc Networks. ***Tran Van Phuong et al [15]*** proposed a TTM to detect wormhole attacks during route setup procedure by computing transmission time between every two successive nodes along the established path. A wormhole is identified base on the fact that transmission time between two fake neighbors created by wormhole is considerably higher than that between two real neighbors which are within radio range of each other. TTM has good performance, little overhead and no special hardware are required. TTM helps to detect wormhole in Wireless Ad Hoc Networks using AODV routing protocol by calculating & comparing the Round Trip Time between every two successive nodes along that route during route setup protocol. TTM is able to detect both hidden & exposed wormhole attacks, locating the wormhole, requiring no special hardware.

Sun Choi et al [14] proposed an effective method called Wormhole Attack Prevention (WAP) is used without using any specialized hardware. The WAP not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. Simulation results show that wormholes can be detected and isolated within the route discovery phase. We achieve this through the use of the neighbor node monitoring method of each node and wormhole route detection method of the source node on the selected route. Our mechanism is implemented based on the DSR protocol and is proven to be capable through simulation results.

This paper discusses some of the existing defense mechanisms in wormhole detection and also proposes a new algorithm for detecting multiple wormholes in an ad hoc network. ***Revathi venkataraman et al [13]*** proposed a graph theoretic approach based on adjacency matrix of a network is proposed which easily detects the presence of wormholes in mobile ad hoc network. This approach is advantageous since it does not increase the computation complexity in a mobile node which is resource constrained. This paper discusses some of the existing defense mechanisms in wormhole detection and also proposes a new algorithm for detecting multiple wormholes in an ad hoc network. If symmetric links are assumed, the upper triangle of the matrix is sufficient to store all the neighborhood information. The adjacency matrix requires n(n-1)/2 bits of storage. Alternatively, a linear array can be used to represent the set of neighbors of each node in an ad hoc network. Choosing the necessary data structures for neighbor listing and performance analysis of the algorithm is our future work. The mechanism will be accordingly modified to suite reactive protocols also.

For detecting routing misbehavior in MANET's lot of techniques are there such as watchdog, path rater, TWOACK, SACK, End to End ACK scheme. But due to the disadvantages of the above scheme ***Shalini V. Wankhade [12]*** proposed a new scheme called 2ACK and the routing protocol used is Optimized Link State Routing (OLSR). The proposed system is a simulation of the algorithm that detects misbehaving links in Mobile Ad Hoc Networks. The system implements the 2ACK scheme which helps to detect misbehavior by a 2 hop acknowledgment. The 2Ack scheme for detecting routing misbehavior is considered to be network-layer technique for mitigating the routing effects. The 2Ack scheme identified misbehavior in routing by using a new acknowledgment packet, called 2ACK packet. A 2ACK packet is allotted to a fixed route of two hops (three nodes N1, N2, N3), in the direction opposite to the data traffic For routing purpose we have used OLSR protocol. The more troublesome task is to determine the characteristics of a single node. The main reason behind this is the communication is only between two nodes and is not any node's sole act. So, any nodes associated with the misbehaving links should be punished carefully. In the case of a link misbehaving, then any one of the two co-related nodes may be misbehaving in the association. In order to find the characteristics and punish a node, we should analyze the behavior of links around that node. A second case may arise wherein Node N1 floods Node N2 with packets thus causing N2 to drop packets. Hence it is imperative that before we declare a node to be selfish on the basis of the number of packets dropped, we should compute the ratio of number packets received against the number of packets dropped.

In this paper, ***Elhadi M. shakshuki et al [11]*** proposed and implement a new intrusion detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Furthermore, in an effort to prevent the attackers from initiating forged acknowledgment attacks, we extended our research to incorporate digital signature in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. We think that this trade-off is worthwhile when network security is the top priority. In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in our simulation. Eventually, we arrived at the conclusion that the DSA scheme is more suitable to be implemented in MANETs. Here technique used is Digital signature algorithm (DSA), Enhanced Adaptive Acknowledgment (EAACK).

Mobile Ad hoc Network (MANET) is an infrastructure less network. Attacks in MANET are due to unreliability, unfixed topology, limited battery power and lack of centralized control. Enhanced Adaptive Acknowledgement (EAACK) is used to detect misbehavior in the network. The 2ACK algorithm is that it can detect the misbehaving link but technique will not give more security. This limitation is been overcome in this paper. Path Tracing Algorithm (PTA) is used to find the exact misbehaving node. Elliptic Curve Cryptography (ECC) algorithm is used to secure the data while passing through the network. ***R. Praveen Kumar et al [10]*** implemented the protocol on ns2 and examined the performance of ECC, which shows that ECC has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes. Wormhole attack cannot be prevented with DSR protocol so we propose AODV protocol for detecting and preventing of wormhole attack using path tracing approach. Here Technique used is Path Tracing Algorithm (PTA), Elliptic Curve Cryptography (ECC).

Publication and year	**Advantages**	**Disadvantages**
IEEE in 2007[15]	It has good performance, Little overhead, and no special hardware.	Detect wormhole with 100% accuracy only when wormhole length is large enough.
IEEE in (2008) [14]	Synchronization needed only at the source node. Detect both hidden and exposed Attack	Failed to detect false positive alarm.
IJRTE in 2009 [13]	Does not increase computational complexity	Performance Analysis of algorithm
IJSETR in 2012 [12]	Detect route misbehaving links	Hard to determine the characteristics of a single node.
IEEE in 2013 [11]	Higher malicious detection behavior in the network. Does not greatly affect network performance.	Network Overhead occur by Digital Signature.
IJREAT in 2014 [10]	Exact misbehaving node is found using Path Tracing Algorithm Data is secured using elliptic curve cryptography	Wormhole attack cannot be prevented with DSR protocol in path tracing approach

Table 1Review

IV. PROPOSED WORK

In the mobile ad hoc networks, the nodes are communicating wirelessly. In this network, due to limited radio range, the nodes are communicating with help of intermediate routers. In this network all the nodes having similar features and functionality, therefore, they can send, receive and route data. Thus most of the attacker nodes are first join to the network and alter the packets those are passing through them. Using the recovered information from these passing packets is used for deploying attack in mobile ad hoc network. Additionally, that can degrade the performance of the network. In the given approach [11] the network overheads increase due to the digital signature.

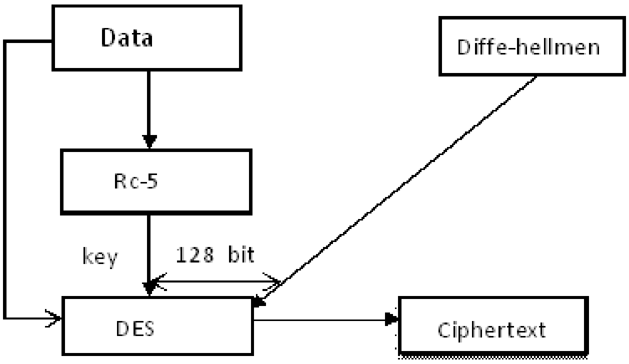

Figure 3 proposed methodology

In order to implement the solution for the distinguished issues in wormhole detection technique, a new solution is proposed. That is a kind of hybrid approach of the traditionally available technique [11] with some additional modification. Therefore, the AODV routing protocol is selected for incorporating the proposed concept. In the

proposed technique first, the route discovery is performed using the traditional AODV routing manner. Where the source node sends the RREQ message and waits for the RREP message reply When the source routing find the shortest path then message data is transmitted using obtained path among source and destination. In order to provide security on data in malicious network data is encrypted using DES algorithm first then after generated cipher text is again processed using the Rc-5 algorithm. The hybrid encryption algorithm designed through the Rc-5 and DES helps to improve the quality of cipher text and now the data packets are ready to send over the network. At the receiver end, the received data is first produced into Rc-5 where decrypted text is again decrypted using the DES algorithm. In addition of that for securing the key exchange process in the network, the DH key exchange procedure is used. Therefore, the proposed security system is an immunity system from the network which is able to deliver the source data at destination node more securely as compared to the traditional methods implemented previously. Finally using the secure key exchange, the designation got a key for recovering the data at the receiver end.

V. CONCLUSION

This paper describes the detailed overview of the MANET and their characteristics. In addition to the different kinds of attacks that are frequently deployed on the network is also explained. Finally, a detailed study on wormhole attack and their types are provided. Furthermore, for detection and prevention, the different available approaches are discussed. Finally using a cryptographic approach, a wormhole avoidance model is proposed for further investigation. This given model is in near future implemented and their performance is computed.

I. REFERENCES

[1] Upadhyay S. and Chaurasia B. K.: Detecting and Avoiding Wormhole Attack in MANET using Statistical Analysis Approach, In the Second International Conference on Computer Science and Information Technology (CCSIT- 2012), Springer, pp. (2012)

[2] Yang H., Luo H., Ye F., Lu S. and Zhang L.: Security in mobile ad hoc networks: challenges and Nsolutions, In IEEE Wireless Communications, vol. 11, no. 1, pp.38–47 (2004)

[3] Zhen J. and Srinivas S.: Preventing replay attacks for secure routing in ad hoc networks, In ADHOC NOW, LNCS 2865, pp. 140–150 (2003)

[4] Hu Y.-C., Perrig A. and Johnson D. B.: Rushing attacks and defense in wireless ad hoc network routing protocols, In W. D. Maughan and A. Perrig, editors, ACM Workshop on Wireless Security (WiSe), pp. 30–40 (2003

[5] B.Revathi & D.Geetha: A Survey of Cooperative Black and Gray hole Attack in MANET, international Journal of Computer Science and Management Research Vol 1 Issue 2 September 2012

[6] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, ―A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks,‖ Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007

[7] Irshad Ullah & Shoaib ur rehman: Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols, Master Thesis Electrical Engineering Thesis no: MEE 10:62 June, 2010

[8] K. Biswas and Md. Liaqat Ali, ―Security threats in Mobile Ad-Hoc Network‖, Master Thesis, Blekinge Institute of Technology‖ Sweden, 22nd March 2007

[9] G. A. Pegueno and J. R. Rivera, ―Extension to MAC 802.11 for performance Improvement in MANET‖, Karlstads University, Sweden, December 2006

[10] R. Praveen Kumar1, A.Excellencia2, P.Kanimozhi3 : Providing a New EAACK to Secure Data in MANET, IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014.

[11] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami : EAACK—A Secure Intrusion-Detection System for MANETs, IEEE Transactions on industrial electronics, vol. 60, no. 3, march 2013

[12] Prof. Shalini V. Wankhade : 2ACK-Scheme: Routing Misbehavior Detection in MANETs Using OLSR, International Journal of Science, Engineering and Technology Research (IJSETR)

[13] Revathi Venkataraman, M. Pushpalatha, T. Rama Rao2 and Rishav Khemka : A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile Ad Hoc, Networks International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009

[14] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung : WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing in 2008

[15] Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Lee : Transmission Time-based Mechanism toDetect Wormhole Attacks, IEEE Asia-Pacific Services Computing Conference in 2007

[16] Akansha Shrivastava and Rajni Dubey: Wormhole Attack in Mobile Ad-hoc Network::A Survey, International Journal of Security and Its ApplicationsVol.9, No.7 (2015), pp.293-298

[17] Manju Ojha1, Rajendra Singh Kushwah : Impact and Performance Analysis of Wormhole Attack on AODV in MANET using NS2, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358 Sannella, M. Ilyas, ―The Handbook of Ad Hoc Wireless Networks, CRC Press, 2003.

CITE AN ARTICLE

Rajput, Malvika , and C. P. Singh, Asst. Prof. "A SURVEY ON WORMHOLE DETECTION AND PREVENTION APPROACH ." *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY* 6.8 (2017): 192-99. Web. 5 Aug. 2017.