International Journal of Research in Advent Technology, Vol.5, No.8, August 2017
E-ISSN: 2321-9637
Available online at www.ijrat.org

A Review of Wormhole Attacks for IEEE 802.11networks

Parminder Kaur[1], Pankaj Kumar Verma[2], J.S. Sohal[3]

Research Scholar[1], Department of Computer Science & Engineering.
Associate Professor[2], Department of Computer Science & Engineering, NIILM University, Kaithal.
Director[3], Ludhiana College of Engineering & Technology, Katani Kalan, Ludhiana.
Affiliated to IKG Punjab Technical University, Jalandhar

Email: pparminderksaini@gmail.com[1], justpankajverma@gmail.com[2], jssohal2001@yahoo.co.in[3]

Abstract: Mobile Ad hoc network (MANET) is a special kind of network where users can join and can communicate anytime, anywhere on the fly. It is an infrastructure free wireless network. Due to its wireless transmissions a number of security and scalability issues affect MANET. Despite the fact that *open standard, dynamic topology, scattered arrangements and multi-hop routing* are the best features of Adhoc Network but if you look in to the security part, then the same features become a biggest threat to the security of MANETs. Due to these features, this type of network is susceptible to various attacks. Wormhole is one of the serious kinds of attack in the Ad hoc Network. Since IEEE 802.11 type of network is quite vulnerable to various types of attacks security becomes the most important issue. This paper presents review of Wormhole attacks for IEEE 802.11 networks.

Index Terms: Attack, Ad hoc Networks, IEEE 802.11, IEEE 802.3, Wormhole.

1. INTRODUCTION TO IEEE NETWORKS

Following are the two different types of Networking Standards provided by IEEE:

1.1 IEEE 802.11:

A technology developed, upgraded and maintained by the Institute of Electrical & Electronics Engineers (IEEE) for Wireless (infrastructure less) network for LAN and MAN. It is a set of Media Access Control (MAC) and Physical Layer (PHY) specifications for implementing Local Area Network, specifically for wireless devises. It is also called WLAN.

1.2 IEEE 802.3:

Another standard made by Institute of Electrical & Electronics Engineers (IEEE) particularly for Wired network. It has defined the Physical Layer and Data Link Layer Media Access Control (MAC) of Wired (infrastructure based) network, such as Ethernet Hubs, Routers, Switches etc. It is frequently used in Local Area Network (LAN). Through this technology physical connections are mounted among various workstations through the specific cables.

The paper is organized as follows: Section 2 describes wireless Ad hoc Network and MANET. Section 3 describes Attacks on Adhoc Network. Wormhole attack is explored in Section 4. Section 5 presents previous work and proposed work. Conclusion & Future Scope of Work is presented in 6 Section.

This paper will be focused on IEEE 802.11 network only.

2. WIRELESS ADHOC NETWORK & MANET

2.1 Adhoc Network:

Ad hoc setup is unlike Client Server setup where all the rights are reserved with Administrator, while in Adhoc wireless network its built impulsively 'as and when' devices communicate with each other. It is a special type of peer to peer wireless network approach where wireless devices transfer data among each other directly without Wireless Access Point device. In Adhoc network these devices should preferably be within local range of each device with whom it has to communicate (Figure-1). But when more devices are added to the network, quality of connection as well as speed of the network becomes poor. The security of an Ad hoc network is non-existent, because wireless security norms are not permitted in such extemporaneous networking.

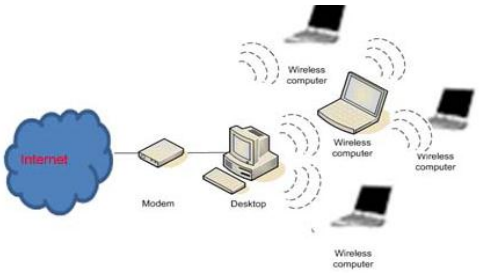

Figure 1- Wireless devices transfer data directly.

2.2 Types of Wireless Ad hoc networks

The various types of Ad hoc networks are (Figure-2):

2.2.1 Wireless Mesh Network.
2.2.2 Wireless Sensor Network.
2.2.3 Mobile Ad hoc Network.

2.2.1 Wireless Mesh Networks (WMN):
WMN is a network of radio nodes structured in a Mesh topology that communicates within the mesh but is unable to communicate the internet. The clients within the network are usually wireless equipments (i.e. Phones, Laptops and Mobiles etc.). They transmit data using Gateways and Routers.

2.2.2 Wireless Sensor Networks (WSM):
It employs sensor based devices to jointly detect environmental & physical settings like climatic changes, sound or pressure etc. used in areas like: vehicle detection system, traffic control system or monitoring system etc.

2.2.3 Mobile Ad hoc Networks (MANET):
It is a self-forming network of mobile devices connected remotely without any infrastructure.

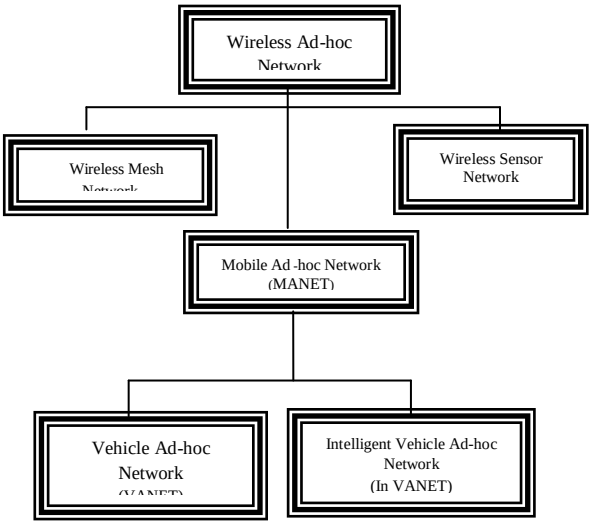

Figure 2- Types of Wireless Ad hoc Networks.

MANET is very popular because its applications cover a variety of areas [1]. It is self-organized and self-managed network. MANET is very famous due to the fact that these networks are dynamic and without any infrastructure. By nature it is an independent and flexible network that is able to execute without centralized administration (unlike Client Server Network). In MANET all nodes act in a Co-operative manner. For example; each device in MANET needs to forward traffic that is not related to its own use and therefore each device works as a Router [2] to transfer packets towards destination. Many more characteristics are there which affects MANET that will be discussed later.

2.2.3.1 Characteristics of MANET:

Wireless Ad hoc network has variable properties which are as under:

- ✓ Network Scalability.
- ✓ Quality of Service (QoS).
- ✓ Energy constrained operation.
- ✓ Dynamically changing network topologies.
- ✓ Variation in Link and Node Capabilities.
- ✓ Infrastructure less capability.
- ✓ Network Security.
- ✓ Autonomous behavior of node.
- ✓ Distributed operation.
- ✓ Multi hop Routing.
- ✓ Light weight terminals.
- ✓ High user density and large level of user Mobility [3].

The self-supporting nature of Ad hoc network makes it quite useful in quick transfer of information between two computers like in natural disasters or emergency military operations etc. Along with all advantages in the day to day life, there are various physical and performance restrictions of Ad hoc network. Despite the fact of the popularity of MANET, these networks are fully exposed to attacks [4, 5].

Due to its self-organized nature, implementation of security in a Mobile Ad-hoc Network becomes very important issue. A few security issues are discussed below:

(a) Availability: Availability applies both, to the Data and Services. It ensures that the devices are accessible to authorized parties at appropriate times. It also ensures the survivability of network service despite Denial of Services (DoS) attacks. Information only has value if it is being accessed at the right time.
Denying access to information has become a very common attack now days, e.g. High profile

websites are being taken down by DDoS Attacks [26]. Therefore, availability is very serious issue of MANET.

(b) **Confidentiality:** Confidentiality ensures that only the right people can read the information. Data should be protected against any disclosure attack like Eavesdropping Attack i.e. unauthorized reading of messages. Through "Data Encryption" schemes confidential data can be protected from the unauthorized users.

(c) **Integrity:** Integrity ensures authorized way to assess resources. Integrity ensures that a message being transferred is never corrupted. Information only has a value if it is correct. The information that has been tampered with would either prove expensive or may not be useful for the end users. Integrity involves maintaining accuracy as well as consistency of data during its complete life cycle. Cryptography is helpful in ensuring data integrity.

(d) **Authentication**: This process confirms and validates user's identity that the resources of network should be accessed by the valid nodes only. The use of Biometrics for finger prints and digital certificates issued and verified is an example of authentication.

(e) **Authorization:** This security technique is used to determine rights to the users to access resources like workstations, services, applications, data or files etc. This property is capable to assign different rights to different types of users. During authorization, a system verifies an authenticated user.

(f) **Freshness:** Freshness guarantees that the information obtained from nodes is recent and not a reply of old data packet [6, 7], because malicious nodes can also resend previously captured packets.

(g) **Resilience to Attacks:** No System or Network is foolproof. Network Security Resiliency is a plan for how to protect data from attacks. It is required to sustain the network functionalities when a portion of nodes is destroyed. Ensuring network resilience through real word testing, using Attack Modules or Real World Malware is the best solution.

To implement security above mentioned issues have to be measured in MANET.

3. ATTACKS ON AD HOC NETWORK

It has been seen that, day by day Ad hoc network is attaining popularity for distributed applications. Subsequently, it is also very important to mention that network is very prone to various kinds of attacks [8] that are mentioned below:

3.1. Attacks on Internet Connectivity [9]:

- Bogus Registration.
- Forged FA.
- Replay Attack.

3.2. Attacks on Mobile Ad hoc Networks [9]:

- Black Hole Attack [10, 11].
- Blackmail Attack[12].
- Byzantine Attack [13].
- Cloning Attack [14].
- Colluding Misrerlay Attack [15].
- Denial of Service Attack [16].
- De-synchronization Attack.
- Eavesdropping Attack.
- Fabrication Attack.
- Gray Hole Attack [17].
- Flooding Attack [15].
- Impersonation Attack.
- Jamming Attack [17].
- Link Spoofing Attack.
- Link Withholding Attack [17].
- Malicious code Attack.
- Man-in-the-middle Attack [18].
- Modification Attack.
- Node Isolation Attack.
- Overwhelm Attack.
- Replay Attack.
- Resource Depletion Attack [19].
- Routing Attack [19].
- Repudiation Attack.
- RERR Generation Attack.
- Routing Table Poisoning Attack.
- Rushing Attack [17].
- Selective Forwarding Attack [20].
- Selfish Misbehavior of Nodes.
- Session Hijacking Attack.
- Sleep Deprivation Attack [12].
- Snare Attack.
- Snooping Attack [21].
- Sybil Attack.
- SYN Flooding Attack.
- Invisible Node Attack.
- Traffic Analyze Attack [22].
- Wormhole Attack [16].

Last but not the least, 'Wormhole Attack'. One of the most challenging attacks to defend against is the Wormhole Attack.

4. WORMHOLE ATTACK

In Wormhole attack, the attackers introduce fake nodes to replay the data and control packets from one location in a network to another location through a link (also called Tunnel). That location can be far away from each other (i.e. several hopes), but yet the nodes will be strongly connected with IEEE 803 or IEEE 802.11 type of network and will transfer datagrams at very high speed. These strongly connected fake nodes (also called malicious nodes [23]) are controlled by the attacker silently without disclosing the facts to any other legitimate node in the Ad hoc Network, because the main aim behind these attacks will be to draw high traffic through the Wormhole and disrupt routing of the legitimate nodes.

In Wormhole attack the effect of attack highly depends upon the position of both the colluding attackers [24]. When the Wormhole attacks are used by attacker in routing protocol such as AODV (Ad hoc On-demand Distance Vector) and DSR (Dynamic Source Routing) protocol, the attack could prevent the discovery of any route other than through the Wormhole [25].

Wormhole Attack categorized under Denial-of-Service Attacks (DoS) [26] attacks (Figure-3).It affects network routing, and especially location based wireless security [27].

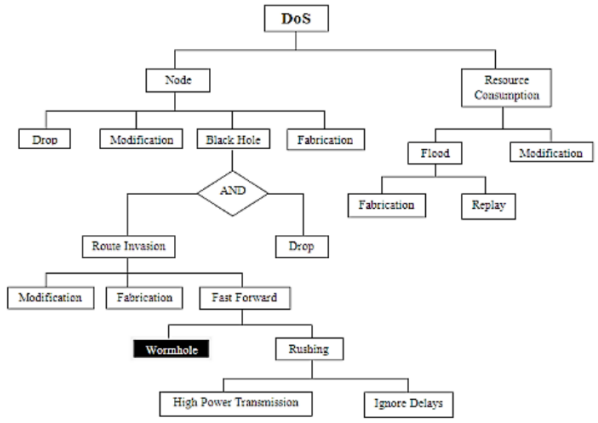

Figure 3: Denial-of-Service Attack (DoS) Tree.

4.1 Wormhole Tunnel: A link of fake nodes frequently launches Wormhole Attack by occupying strong locations in two different parts of the Ad hoc network by occupying main stations in a network. These nodes will misleadingly advertise to the neighbour nodes that they are having shortest path for the destination. Internally these malicious nodes will create a tunnel to transfer data packets to some other private network of IEEE 802.3 type of network and that private network will have very high transmission speed. Figure-4 represents the Wormhole Tunnel, in which node **'A'** and node **'P'** are two malicious nodes and are making a tunnel (Wormhole tunnel) bye passing the main pathway. Therefore; as a

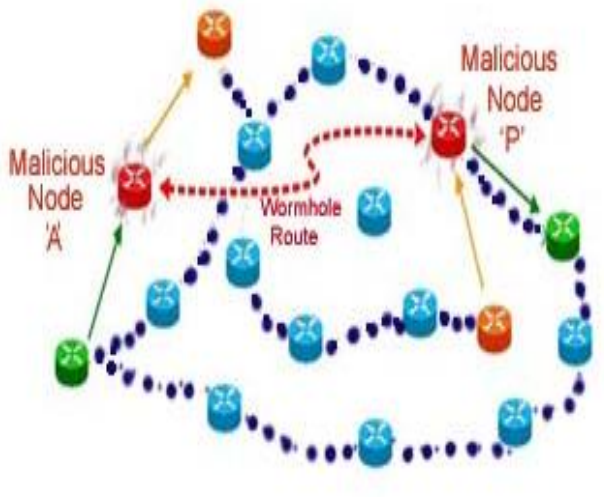

Figure 4- Wormhole Tunnel.

result either most of the data will be dropped or forwarded to some other place by these malicious nodes through the above mentioned tunnel. In few circumstances data may also be tampered by these Malicious Nodes.

5. PREVIOUS WORK &PROPOSED WORK

5.1 Previous Work:

Simulation of security strategies provides the facility to select a good security solution for routing protocols. To defeat the opponent and to overcome the above mentioned problems of Wormhole Attack, various detection techniques have been used by the researchers. These detection techniques are:

5.1.1 Time Based Mechanisms [28, 29, 30].

5.1.2 Deploying Directional Antennas [31].

5.1.3 A design of two protocols capable of detecting a Wormhole Attack at the receiver end presented by Y. C. Hu et. a1. [32, 33].

5.1.4 Hop Count [34], [8] analysis approach has also been proposed by **Kirti Patidar** et al. [35].

5.1.5 The Slot Authenticated MAC protocol and the TIK [36] protocol, both protocols rely on Tight Time Synchronization. Time Synchronization is again a major problem for IEEE 802.11 network.

5.1.6 **Ajay Jangra** et. al. proposed EPSAR (Efficient Power Saving Adaptive Routing Protocol) which is a novel approach for the selection of farthest and efficient node within the clusters. EPSAR used AODV & DSDV. In order to get reliable and efficient path in multi-hopping EPSAR is followed. The technique tried to find out the actual working with different parameters like unreliable battery, malicious node. FRENSA is the basic concept of EPSAR [37].

5.1.7 **A. K. Sharma** et. al. proposed a novel algorithm for selecting best neighbor node in multicast MANETs named BNNSA (Best Neighbor Node Selection Algorithm) [38].

5.1.8 **Alexandros** et. al. evaluated multicasting algorithms for MANETs. Multicasting is used for one to many and many to many node communications. Performance of MAODV (Multicast Ad Hoc On Demand Distance Vector Routing Protocol) and ODMRP (On Demand Multicast Routing Protocol) are evaluated on the basis of packet delivery ratio and latency. It has been observed from MAODV that it performs well in large areas while ODMRP performs much better in high speed [39].

5.1.9 **Dimple Saharan** proposed a solution to prevent the network against wormhole attack through a Secret Key for encryption and decryption of hello packets, to deal with only authentic nodes. It has been done through AODV as routing protocol. As a result communication can take place only between the trusted nodes [40].

5.1.10 **Jen** et al. proposed a novel scheme based on an intuitive method to avoid Wormhole Attacks in MANET from the viewpoint of users instead of administrator as in previous work.

The proposed scheme has high efficiency and good performance with low overhead without using additional hardware or impractical assumptions of the network [41].

5.1.11 **Johnson** et al. presented working of protocol. A key reason for this good performance is the effect that DSR operates entirely on demand with no periodic activity. These two special properties of DSR allow the number of routing overhead packets (caused by DSR) to scale all the way down to zero, when nodes are approximately stationary with respect to each other and all routes are waiting for current communication that already been discovered [42].

5.1.12 **Kimaya Sanzgiri** et. al. proposed a certificate based protocol named ARAN to reduce security threats to AODV & DSR and tries to avoid all identified attacks. Author discussed about different activities which are possible against routing protocol in Ad hoc network and identified various security environments with their varying requirements and security threats. They explored in detail security requirements of Ad hoc networks and finally proposed a secure routing protocol for managed open environment that put any extra work load on the nodes of the network but still prevent the network from many security threats. Simulation study proves efficiency of the proposed protocol [43].

5.1.13 **Madhavi** et. al. proposed an intrusion detection system named MIDS (Mobile Intrusion Detection System) for Multi-hop Network. This system detects the misbehavior of nodes, packet drop in network and delay by appointing a monitor in the network very efficiently [44].

5.1.14 **Priyanka** et. al. introduced a Nod selection algorithm named FRENSA (Farthest Reliable Efficient Node Selection Algorithm), works on multi-hopping mechanism. FRENSA is designed for next node selection and to enhance the quality of network. It selects the next node with respect to distance from sender node. It is popular for power backup and reliability for packet forwarding. This criterion reduced the overall communication head and improves the reliability of the network [45].

5.1.15 **Sharif** et al. proposed a wormhole detection technique which makes use of AODV as an On Demand Routing Protocol and Secure Neighbour Detection Protocol with certain modification. During analysis of the reply message, sender confirms the number of routes by sending packets of verification to individual

nodes whose identification has been stated by receiver and based upon the delay in time wormhole link is detected. The periodic exchange of information among the neighbors validates the Ad hoc network reliability. Analysis provides that the proposed technique not only detects the wormhole link but also provides a verification mechanism to judge the validity of nodes. Therefore, the proposed technique was capable of ensuring Ad hoc network's security where wormhole attacks ratio is high [46].

5.1.16 **Yi** et. al. introduced a new protocol named MOCA (MObile Certificate Authority) based on PKI (Public Key Infrastructure) and CA (Certificate Authority) proposed for efficient communication [9].

5.1.17 **Zubair** et al. proposed the use of the modified Routing Table for detection of the suspicious links, confirmed of wormhole existence and isolating the confirmed wormhole Nodes. The approach has been applied to DSDV and the detection of self-sufficient Wormhole nodes and attacks. The initial study showed that an approach can be incorporated that use this information for the detection of Wormhole links [47].

Accordingly, it is concluded that due to dynamic topology MANET has no centralized monitoring and has limited physical security. Following points are inferred from the survey:

- These devices are very limited in resources and need many solutions for better working of these devices.
- Protocols are vulnerable to attacks and Wormhole Attack is one of them that need improvement.
- In MANET there is a need to detect and prevent the other various attacks also.
- Many solutions are there but due to dynamic nature, these problems keep on rising and need more updated solutions as per the current scenario of MANET.

Previously detection technique used Hope Count Analysis approach based on Hop Count Value [48] that was error prone and may create problem because, deriving distance estimates from Hop counts is prone to error (Error types may be underestimation or overestimation of distances in MANET). This leads to an unpredictable underestimation which can result in a negative error.

As per base paper (i.e. 5.1.4) **Kirti Patidar** et al. proposed protocols to protect Ad hoc networks from Black hole & Wormhole attacks and to improve network stability. This presents an 'Intrusion Detection System' based on the concept of Specification-Based Detection System to detect and prevent Black hole attack.

Base paper also presents Hop count analysis approach to detect Wormhole attacks along with routes in Ad hoc networks. The proposed protocol does not require any location information, time synchronization or special hardware to detect Wormhole attacks.

Given below simulation parameters are taken from the base paper for topology design and analyzed the results according to PDR, Throughput and Delay.

According to the base paper protocols are evaluated using analysis and simulations on Network Simulator version 2.35.

Simulation Parameters	
Channel	Channel/Wireless
Propagation	Propagation Two Ray Ground
Network Interface	Phy/Wireless Phy
Platform	Ubuntu 16.04
NS Version	Ns-allinone-2.35
Mac	Mac/802_11
Interface Queue	Queue/Droptail/ Pri queue
Link Layer	LL
Antenna Antenna/	Omni Antenna
Interface Queue Length	50
No. of nodes	5_10_15_20_25
Simulation Area size	750*550
Traffic pattern	CBR Sessions
CBR packet size	512 bytes
Simulation Duration	32 Seconds
Protocol	AODV

5.2.1 Proposed Detection Technique:

For Wormhole detection, it is necessary to find out Tunnel between the nodes. In the proposed technique, first of all a Tunnel between the nodes **are** identified and then Wormhole attack is detected using proposed technique in the selected Ad hoc Network. **This method first checks the variable of 'Routing Table'** to know the entry of all nodes, because as per the genuine procedures, every node in the network **is** supposed to

carry out its own Routing Table. It is important to mention here that the same rule of maintaining 'Routing Table Entry' is also applied to the Malicious Nodes.

The important point is to note that Malicious Nodes are **also having** 'Routing Table' but **this** table will have only entry (information) of Malicious Nodes and entry of other remaining nodes **is** missing in the Routing Tables of Malicious Nodes. This 'Routing Table missing entry' is an indication that the node is not legitimate.

By using the above mentioned 'Routing Table Entry' logic all the other nodes can be checked in the particular network. If the subsequent nodes do not have entry in the Routing Table then message **is** conveyed to the Source Node that some attacks are found (e.g. Wormhole) in the network. Now, Source **Node decides** next course of action to forward data, because attempts can **only** be made to secure data from the malicious **nodes after** identifying such Tunnel between Malicious Nodes.

5.2.2 Proposed Prevention Techniques:

In this case new technique **is** applied to prevent Wormhole attack so that data can be transferred successfully from source to destination. After detection of Malicious Nodes, the information of Malicious Nodes **is** recorded. **Now** source node will decide to find out new path instead of previous one, simultaneously it will start searching new path and will select one path from the available paths and will send the data to destination again. This technique will not entertain any Malicious Node to forward data packets, but will use some alternative approach to transfer data efficiently.

5.2.3 Proposed Results:

In the proposed work author has **made an attempt** to get better results as **compared to the Base paper i.e.** "Modification in Routing Mechanism of AODV for Defending Black hole and Wormhole Attacks" [35]. **Results obtained in terms of performance metrics like: PDR, Throughput and Delay vs. Simulation time are improved.**

For MANET topology, it is compulsory to choose at least one Routing protocol [49, 50]. Therefore; in the proposed work, detection and prevention of wormhole attacks **is** carried out by using Ad hoc On-demand Distance Vector (AODV) Routing protocol. No special hardware **is** being required. NS2 [51] Simulation Environment **is used like** Simulator, Data Extraction & Reporting Tool, Scripting Language for configuration and Programming **Language on a 64 bit** Operating System.

In specific the following **factors support** the simulation environment in the proposed work:

- Data Extraction & Reporting Tool -Awk
- Scripting Language for configuration -Tcl Script
- Programming Language - C++
- RAM - 4GB
- O/S Type - 64 Bit

6. CONCLUSION & FUTURE SCOPE OF WORK

It has been discussed that MANET is vulnerable to various attacks. A survey of various literatures on Wormhole attack has been performed. Flaws of MANET are also explored. It has been observed from the Literature Review that Attacks are the biggest threat in MANET, those threats are discussed and subsequently effects of Wormhole Attack that needs improvement has also been discussed.

It is concluded that Ad hoc Network is highly prone to Wormhole Attack and Simulation of security strategies provides the facility to select a good security solution for routing protocols.

REFERENCES

[1]. Raja Datta, Ningrinla Marchang, "Security for Mobile Ad Hoc Networks", Handbook on Securing Cyber-Physical Critical Infrastructure. DOI: 10.1016/ B978-0-12-415815-3.00007-8 147, 2012, Science Direct-Elsevier.

[2]. Gunjesh Kant Singh, Amrit Kaur and A.L. Sangal, "Performance Analysis of DSR, AODV Routing Protocols based on Wormhole Attack in Mobile Ad-hoc Network", 5th International Conference on Advanced Computing & Communication Technologies [ICACCT-2011] ISBN 81-87885-03-3-2011, IEEE.

[3]. Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Applications and Security Attacks", International Journal of Advanced Research in Computer Science & Software Engineer, Vol. 3, Issue 5, pp. 252-257, ISSN:227128X, May 2013.

[4]. Y. F. Alem, Z. C. Xuan, "Preventing Wormhole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May, 2010.

[5]. M. Parsons, P. Ebinger, "Performance Evaluation of the impact of Attacks on Mobile Ad-Hoc Networks", April. 2010.

[6]. Satyabrata Chakrabarti (Lucent Technologies), Amitabh Mishra (Virginia Technologies), "QoS issues in Ad Hoc Wireless Networks", Communications Magazine, February 2001 , pp: 142-148, IEEE.

[7]. Eric Cole, Ronald L. Krutz, James W. Conley, Brian Reisman, Mitch Ruebush, Dieter Gollmann, "Network Security Fundamentals", ISBN: 978-0-470-10192 -6, 2008.

[8]. Ning P, Sun K., "How to misuse AODV: a case study of insider attacks against Mobile ad-hoc routing protocols", in proceedings of the IEEE systems, Man and Cybernetics Society Information Assurance Workshop (IAW), West Point, New York, USA, 2003. pp. 60–7, IEEE.

[9]. Seung Yi, Robin Kravets "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks", University of Illinois at Urbana-Champaign Urbana, IL61801.

[10]. Ashish Kumar Jain, Vrinda Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile Ad hoc Networks", Pervasive computing (ICPC), 2015, International Conference on IEEE.

[11]. Kishor Jyoti Sarma, Rupam Sharma, Rajdeep Das, "A Survey of Black Hole Attack Detection in MANET", IEEE, 2014.

[12]. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal of Computing, Vol. 3, Issue 1, January 2011, ISSN 2151-9617.

[13]. Nigahat, Dr. Dinesh Kumar, "A review on Black hole attack in Mobile Ad-hoc Networks", International Journal of Engineering Sciences & Research Technology, 82-2017.

[14]. D Sheela, G. Mahadevan, "Mollifying the effect of Cloning, Sink Hole and Black Hole Attacks in Wireless Sensor Networks using Mobile Agents with Several Base Stations", International Journal of Computer Applications, pp. 0975 – 8887, Vol. 55– No.9, October 2012.

[15]. Rishabh Jain, Charul Dewan, Meenakshi, "A Survey on Protocols & Attacks in MANET Routing", International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012 ISSN: 2231 –5268.

[16]. Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications (0975 – 8887) Vol. 9, No.12, November 2010.

[17]. Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology, ISSN: 2249 – 8958, Vol.1, Issue-5, June 2012.

[18]. Sharad Awatade, Pankaj Chandre, "Detection and prevention of attacks on MANETS using advanced EAACK and hybrid key cryptography", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Vol. 4, Issue-1, Jan 2016.

[19]. Jan von Mulert, lan Welch, Winston K. G. Seah, "Security threats and solutions in MANETs A case study using AODV & SAODV", Vol. 35 (2012), pp 1249–1259, Science Direct- Elsevier.

[20]. Manjeet Singh et. al., "A Surveys of Attacks in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 6, June 2013, ISSN: 2277 128X.

[21]. Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET- Internet Communication", International Journal of Computer Science and Security, Vol. 4, Issue 3.

[22]. A. GOPI, DR. A. Nagesh, Pavan Srinivas, "The Analysis of Security Challenges in MANETS", International Journal of Advanced Scientific and Technical. Research Issue 7, Vol 1, pp 310-322, ISSN 2249-9954, January –February 2017.

[23]. Ming-Yang Su, "WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks", Computers & Security, Vol. 29 (2010), 208 – 224, Science Direct-Elsevier.

[24]. Ankita M. Shendurkar1, Prof. Nitin R. Chopde2, "A Review of Black Hole and Wormhole Attack on AODV Routing Protocol in MANET", IJETT, Vol. 9, Number 8, pp 394, Mar 2014, ISSN: 2231-5381.

[25]. Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", IJEAT, Vol-1, Issue-5, ISSN: 2249 – 8958, June 2012.

[26]. Abdelaziz Amara Korba, Mehdi Nafaa, Salim Ghanemi, "An efficient intrusion detection and prevention framework for ad hoc networks", Information & Computer Security, 2016- Vol. 24 Issue: 4, pp.298-325.

[27]. M. Meghdadi, S. Ozdemir and I. Guier, "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", IETE Technical Review, Vol. 28, Issue 2, pp 89-102, 2011.

[28]. X. Su and R. V. Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks", in

Proceedings of IEEE Communications Society, ICC 2007.

[29]. P. V. Tran, L. X. Hung, Y. K. Lee, S. Lee and H. Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", IEEE, pp 593-598,2007.

[30]. T. V. Phuong, N. T. Canh, Y.K. Lee, S. Lee and H. Lee, "Transmission Time-based Mechanism to Detect Wormhole Attacks", IEEE Asia-Pacific Services Computing Conference, Computer Society, pp 172-178, 2007, IEEE.

[31]. L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", In Network and Distributed System Security Symposium - 2004, San Diego, California, USA. February 2004.

[32]. Y.c. Hu, A. Perrig and D. B. Johnson, "Wormhole Detection in Wireless Ad Hoc Networks", Technical Report TROI-384, Rice University Department of Computer Science, 2002.

[33]. Y.c. Hu, A. Perrig and D. B. Johnson, "Wormhole attacks in wireless networks", IEEE Journal on selected areas in communications, Vol. 24, No. 2, 2006.

[34]. M. Devi, Dr. G. Kesavaraj, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks", IJCSE, 11-03-06-040.

[35]. Kriti Patidar, Vandana, Dubey, "Modification in Routing Mechanism of AODV for Defending Black hole and Wormhole Attacks", 978-1-4799-3064-7/14/S 31.00 © 2014 IEEE.

[36]. Yih Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", 2003, IEEE INFOCOM.

[37]. Ajay Jangra, Nitin Goel & Priyanka, "Efficient Power Saving Adaptive Routing Protocol (EPSAR) for MANETs using AODV and DSDV: Simulation and Feasibility Analysis" in IEEE, IPTC 2011.

[38]. A.K. Sharma and Amit Goel, "Best Neighbor Node Selection Algorithm for MANET", Journals of Institution of Engineers, Jan 2005.

[39]. Alexandros Vasiliou et al, "Evaluation of multicasting algorithm in MANETs", in Proceedings of World Academy of Science, Engineering and Technology, Vol. 5, April 2005, ISSN 1307-384.

[40]. Dimple Saharan, "Detection & Prevention of Wormhole attack on AODV Protocol in Mobile Adhoc Networks", IJECS, Vol. 3, Issue 9, September, 2014, pp.7979-7985.

[41]. Jen, Chi Sung liah, Wen Chung Kuo, "A Hop count Analysis for Avoiding Wormhole Attacks in MANET", Sensors 2009, Vol. 9, pp 5022-5039, DOI: 10.3390/s 90605022, ISSN: 1424-8220.

[42]. Johnson Yih Chun Hu, Adrian Perrig, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", INFOCOM, 2003, IEEE.

[43]. Kimaya Sanzgiri, Bridget Dahill, Brain Neil Levine, Clay Shields and Elizbeth M. Belding-Royer, "A secure routing protocol for Ad Hoc Networks", Proceedings of 10th International Conference on Network Protocols (ICNP' 02), 2002, IEEE.

[44]. Madhavi, Tai Hoon Kim, "An Intrusion Detection System in Mobile Ad hoc Networks", International Journal of Security and its applications, Vol. 2, No. 3, July 2008.

[45]. Priyanka, Komal Kumar Bhatia, Ajay Jangra "FRENSA: Farthest, Reliable and Efficient Node Selection Algorithm for Mobile Ad-hoc Networks", in IJCST International Journal of computer Science and Technology, Vol. 1, Issue 2, December 2010.

[46]. Sharif, Aisha Azeem, Mudassar Raza Waqas Haider, "A novel Wormhole Detection Technique for Wireless Ad Hoc Networks", International Journal of Advanced Network and Application, Vol. 3, Issue 5, pp 1298-1301, 2012.

[47]. Zubair Ahmed Khan, M. Hasan Islam, "Wormhole attack: A New Detection Technique", 2012, IEEE.

[48]. Sabrina Merkel, Sanaz Mostaghim, Hartmut Schmeck, "Hop count based distance estimation in Mobile ad hoc networks – Challenges and consequences", Ad Hoc Networks 15 (2014), pp 39–52, 1570-8705/$ - see front matter - 2013, Science Direct – Elsevier.

[49]. Arun Kumar et. al., "A Survey of Mobile Ad Hoc Network Routing Protocols", Journal of Intelligent System Research, pp. 49-64, Serials Publications, New Delhi, 2008.

[50]. Vijaya et. al., "Influence of Routing Protocols in Performance of Wireless Mobile Adhoc Network", Second International Conference on Emerging Applications of Information Technology, DOI 10.1109/EAIT.2011.65, 978-0-7695-4329-1/11 $26.00 © 2011 IEEE.

[51]. T. Issariyakul and E. Hossain**,** "Introduction to Network Simulator NS2", 2009, Springer.