ADDRESSING THE DISTINCT SECURITY VULNERABILITIES TYPICALLY EMERGE ON THE MOBILE AD-HOC NETWORK LAYER

[1]Gaurav D Saxena
Department of Computer Science, Kamla Nehru Mahavidyalaya, Nagpur, Maharashtra, India
E-mail: gauravsaxena@kamlanehrucollege.ac.in

[2]Dr.Dinesh G
Assistant Professor, Department of Computational Intelligence, School of computing
SRM institute of science and technology, Kattankulathur, Kanchepuram
E-mail: dineshcsenhce@gmail.com

[3]Dr. D. Stalin David
Department of Information Technology, VelTech Multitech Dr.Rangarajan Dr. Sakunthala Engineering College Avadi, Chennai-600062. E-mail: sdstalindavid707@gmail.com

[4]Mohit Tiwari
Assistant Professor, Department of Computer Science and Engineering,
Bharati Vidyapeeth's College of Engineering, Delhi, A-4, Rohtak Road, Paschim Vihar, Delhi. Mail id : mohit.tiwari@bharatividyapeeth.edu

[5]Tripti Tiwari
Assistant Professor,
Department of Management Studies, BVIMR, A-4, Rohtak Road, Paschim Vihar, Delhi.
Mail id : tripti.tiwari@bharatividyapeeth.edu

[6]Dr. M. Monisha
Assistant Professor, Department of Electronics and Communication Engineering,
Vels Institute of Science Technology and Advanced Studies – VISTAS, Pallavaram, Chennai – 117. E mail - monish.ece147@gmail.com

[7]Dr. Amit Chauhan
Assistant professor, Department of Life sciences, CHRIST (Deemed to be university),
Bangalore, Karnataka-560029, India. E-mail: amit_chauhan777@yahoo.in

Abstract

An ad-hoc network, also called a mobile or wireless local area network (WLAN), uses a dynamic structure in which nodes are connected without the need for any fixed infrastructure. These networks can be setup anywhere, and often consist of individual devices such as smart phones that are roaming together to form a larger network. What is the name for this type of networking? The term "mobile ad-hoc network" (MANET) is typically used to describe these types of networks that involve Mobile Hosts. One of the biggest challenges in designing a networked system is maintaining communication between nodes. This can be difficult because nodes are often randomly located, and they may join or leave the network at any time. Because MANETs rely on this decentralized structure, they are more vulnerable to attacks than wired networks. As a result, security becomes an important concern for the network—and it is essential that messages be sent securely so that communications remain uninterrupted. In this paper, we have surveyed attacks that can occur at the network layer of a protocol stack in MANETs. The aim of our work was to provide an overview of all types of attack on networks layer on MANET Protocol stacks, which will help us better understand how these attacks may be applicable to MANETs. We hope that by doing so, we will be able to classify all such attacks and identify any potential weaknesses or vulnerabilities in protocols used for networking within MANETS.

DOI Number: 10.48047/NQ.2023.21.3.NQ33019 **NeuroQuantology2023;21(3): 169-178**

1. Introduction

Owing of the threat that mobile devices could pose to people and organizations, wireless communication has recently received attention as a research area. Network security is one of these concerns; how can one ensure that wireless network nodes are immune from attacks? This problem exists because networks without infrastructure support (like MANETs) are continually changing and growing, making it difficult for attackers to get a foothold. These networks' nodes are open to various assaults that might lead to their theft or annihilation. In order to ensure node security in this setting, researchers have been working hard.[1-4] The way an intruder is dealt with differs between infrastructure-based wireless networks and wired networks. In a wired network, the invader is often someone external to the system who can be managed by a firewall. This makes it simpler to recognize them and impose access restrictions. On the other hand, we must take into consideration users who are already connected to the network, or invaders, while constructing a wireless network. Because they are already a part of the network and lack any external connections that would make them stand out from the rest, intruders on MANETs might be more challenging to identify. Therefore, this distinctive feature of MANETs may make spotting aberrant activity tougher than usual.[5] Network operation is highly concerned about security. By taking action to make sure security has been taken care of, network services are available, data is private, and integrity is maintained. Although MANETs are vulnerable to assaults because of their characteristics (such as an open medium), dynamically changing topology, absence of centralized monitoring and management, and cooperative algorithms), there are techniques to reduce these vulnerabilities. For instance, by ensuring appropriate security measures have been included throughout the network design process, integrating tools like firewalls or intrusion detection systems, conducting routine threat assessments, and deploying.[6-11] In order to maintain safe communication between nodes, engineers must be aware of the many attacks that may be conducted against mobile networks. Wormhole attack: This type of attack involves sending packets via two or more routers without first going through the desired destination node. Black hole attack: In this kind of assault, a malicious user creates a fake black hole on the network by saturating it with traffic, preventing genuine traffic from getting to where it needs to go. Sybil Attack: A Sybil attacker is someone who tries to use many personas on a network to gain unauthorized access or modify data. Attacks using a flood of data packets are carried out by attackers. [12-18]

2. Challenges in Mobile Ad hoc networks [19,20]

The list of problems below highlights the difficulties that must be solved in a MANET environment: - A MANET's nodes must be capable of doing so securely for it to operate as intended.

Due to their difficulty communicating through wireless networks, the radio group will be overloaded by the quantity of data that they may receive. In contrast, a bound network places limits on who may access it and prevents anybody from exhausting it.

To transfer data between devices, wireless communications employ radio waves. These signals are transmitted on particular channels and are susceptible to interference, including path harm (when the signal follows a harmful path), declining channel quality (which reduces the reliability of transmissions), and slowdown due to congestion (caused in part by increased demand for these channels).

Due to the frequent transmission mistakes in ad-hoc wireless networks, packet losses can be fairly substantial. For instance, wireless channels may experience an unthinkable bit error rate (BER).

Ad hoc systems that organize the primary issues in a certain region frequently govern battery constraints on mobile networks[19]. This implies that nodes linked to the network have a restricted range for sending and receiving information as well as a restriction on the amount of data they can transfer at once.

The key issue is routing since it necessitates network nodes to swiftly alter their routes to meet performance requirements. This occurs as a result of how quickly network architecture may alter as well as varied mobility rates. Furthermore, unicasting and multicasting demand are unstable, making routing challenging[20].

Security is main challenge in MANET, due to its wireless environment. In, MANET the data is transferred between nodes freely, so many attacks are possible in MANET.

The quality of service (QoS) in MANET is important because nodes are required to provide different levels of service depending on the demand. However, providing high-quality service at all times is a difficult task, and networks need to best manage this by controlling which level of service is offered.

3. Characteristics of the secure Ad hoc networks [21-36]

Establishing a secure network system that complies with standardized requirements is security's goal. These stated goals include creating security measures for the network and making sure that standardized practices are followed.

A node consistently offers the service for which it was built. It focuses on protecting against self-centered nodes' Denial of Service assaults. Various nodes disable some network functions in an effort to disrupt or harm the system.

Integrity is the method of ensuring that the message is coming from who it claims to be. There are difficulties like malicious attacks, in which someone tries to alter the data being delivered, and unintentional changing, in which something goes wrong but wasn't intended to. The main distinction between these two situations is intent: in a malicious attack, the assailant purposefully modifies information, whereas in inadvertent modifying, the modification is unintentionally made by a benign node.

Confidentiality: Certain information should occasionally only be available to a certain group of people who have been given permission to do so. Unauthorized people shouldn't have access to or be permitted to possess this confidential details.

Authenticity is a process of verifying whether or not a node is an impersonator. This involves encrypting the codes of each participant in order to secure their identities and prevent them from being impersonated by the adversary. It is essential that all participants are identified and authenticated in this way, as an imposter could misrepresent themselves as a benign entity in order to gain access to confidential information.

Non-repudiation is a mechanism by which the sender and receiver of a message can be sure that it was sent and received correctly. This prevents any ambiguity or dispute over who actually sent or received the information. For example, if one node mistakenly believes they have received an erroneous message, they are able to prove this to other nodes through use of non-repudiation. By doing so, all parties involved will be aware that something went wrong and should take appropriate action based on the new information.

4. Security Attack in MANET layer

There are various types of attacks that can be carried out on different layers within a MANET network.

Table 1: Attacks on the Layer of MANET

Layers	Attacks
Application Layer	Attacks by Virus & Worms, Denial of Service attack
Transport Layer	TCP SYN attack, TCP session Hijacking, Jelly fish attack
Network Layer	Flooding attack, Route Tracking, Wormhole Attack, Link spoofing attack, Sink hole attack, Sybil attack, Byzantine attack, Message fabrication attack
MAC layer	MAC attack, Traffic Monitoring attack, WEP targeting attack, Bandwidth stealth attack
Physical Layer	Jamming attack, Compromised or stolen attack, Malicious message injection attack, Eavesdropping attack

4.1 Network Layer attacks in MANETS

Data is often sent to and from devices in a network via packets. Protocols at the Network layer are used to route these packets via the network. This layer makes sure that all network nodes may reliably exchange information and communicate with one another. A malicious node (or hacker) may obstruct this process by inserting itself into active pathways or using excessive bandwidth. This kind of attack entails altering or obstructing traffic to accomplish certain objectives, such clogging servers or getting access to sensitive information. Because of malevolent activity on networks, there are many distinct sorts of assaults, some of which are more serious than others.

MANET attacks can be broadly classified into four types: Internal Attacks, External

Attacks, Active Attacks, and Passive Attacks.

In essence, external attacks are conducted by someone attempting to get access to a network from outside the network. Additionally, once they get access to the network, they can exploit it by sending forged packets that cause the entire network to a halt.

An internal attack is when someone attempts to harm or take advantage of a network from within. There are two methods for this to happen. The first is for an attacker to enter the network and start connecting with other nodes in an effort to locate holes or flaws they might be able to exploit. The second method occurs when a person obtains access to the system while posing as someone else (such as a dependable person) and begins acting maliciously without being noticed. Since each has an own collection of works, it is challenging to foresee which attacks will happen within vs externally.

Attacks that are passive merely include listening in on or watching as data is exchanged between two parties. Because the perpetrators of these attacks don't alter anything or provide any false information, they might be challenging to identify. Eavesdropping is a type of passive attack when someone listens in on a conversation without actively participating. A different kind of passive attack is traffic analysis, in which the attacker gathers specific data about how users are utilizing the network. These kinds of attacks might be challenging to spot since they frequently go unnoticed.

Network attacks: There are several distinct kinds of network attacks, all of which seek to stop or impair a network's regular operation. An active attack is when a hacker tries to manipulate or tamper with the information being transferred across the network. This can be accomplished in a number of ways, including by interfering with the regular flow of traffic, inserting forged packets inside real ones, deleting crucial packets entirely, or even by exploiting network characteristics.

4.1.1 Black Hole Attack

A hostile node fraudulently claims to have the shortest path to the target during a black hole attack, a form of network attack. As a result, the malicious node is able to prevent other nodes from receiving data packets and ultimately accomplish its goal of interfering with communications. This behavior is motivated by greed since it makes it simpler for the malicious node to monopolies resources when other nodes are prevented from interacting. Black hole attacks are frequently used to try to disrupt communication between two other entities by one entity (the attacker) (the target and defender). Blackhole attackers frequently introduce themselves or assert that they have the fastest route to their goal when they assault another node. Attackers utilize RREP messages with large sequence numbers to trick unwary source nodes into sending data packets to these fictitious destinations. By only choosing messages with low sequence numbers, sources are less likely to notice any inaccurate responses, which results in the transmission of erroneous information alongside correct information and ultimately network interruption. [37]

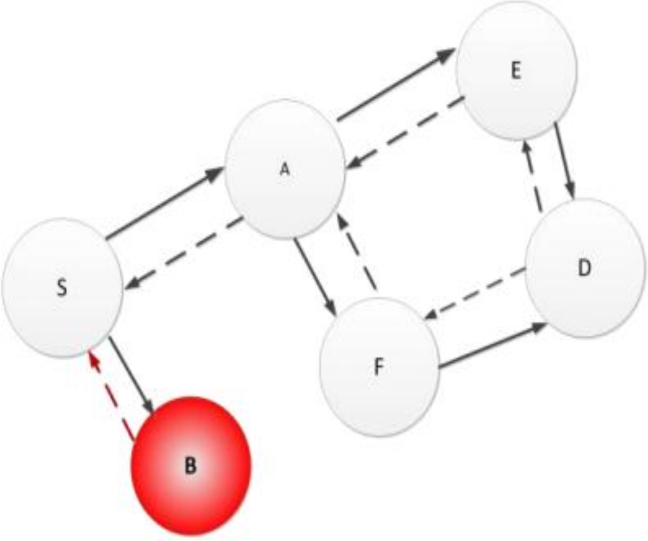

Figure 1: Black hole attack behavior

Figure 1 is an illustration of a black hole attack. The source node S builds a path to the destination node D, but instead broadcasts its RREQ. As it is not the target node, any node that receives this message from the other nodes must forward it. Attacker B sends a counterfeit RREP that says it can get to D more quickly. Nodes will take this message at face value and continue on B's fictitious route towards D since they only receive and process messages that are aimed at them. Data packets sent from the source node S to the destination node D are probably going to be blocked or delayed by the problematic node B. As a result, there may be issues with how the network operates. Malicious node B makes it simpler for nodes 3 and 4 to incorrectly route packets in an effort to reach destination D by raising its traffic load above and above what was initially designed. Both nodes are able to use more resources than necessary as a result, stressing the network.

4.1.2 Wormhole Attacks

A direct tunnel connection is made between two nodes during a wormhole attack. This is feasible by utilising any of the three long-range wireless communication techniques, including cable lines, radio waves, and optical communications. Wormholes can be beneficial in networks with many links between nodes because they offer an alternate path over further distances than would be feasible otherwise. Worms transform into Trojan horses in this fashion, making it simpler and faster for attackers to get over other network segments' security mechanisms. The direct link is typically preferred by naïve nodes over using one of the network's shorter routes to prevent being taken advantage of by such an attack. The exploitation of a wormhole network by malicious nodes for traffic analysis or Denial of Service attacks might be one drawback. They can stop information from moving freely between various areas of the network by discarding specific data or control packets. In order to ensure correct communication, this assault particularly targets routing control packets. The nodes close to the attacker will be protected from any other routes with more than two hops since these packets are transferred from close-by nodes to distant ones.

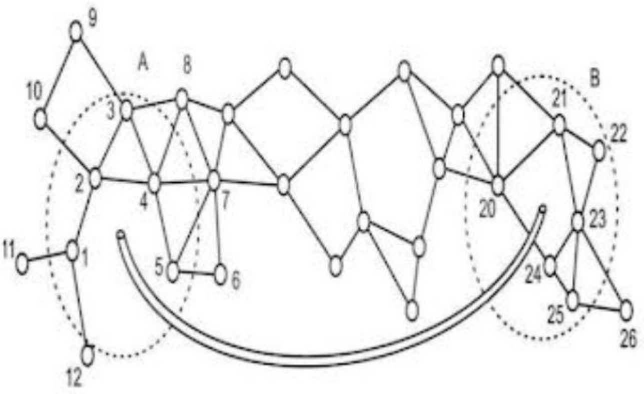

Figure 2: Worm hole Attack

4.1.3 Gray hole attacks

We will now go through the grey hole attack on MANETs. In the initial stage of this attack, a malicious node takes use of the AODV protocol to falsely advertise that it has a legitimate route to a target node. With a certain probability, this enables the malicious node to intercept packets and dump them. The black hole attack, on the other hand, consistently discards every data packet it receives. Due to its reliance on exploitation rather than the random discarding of incoming data packets, the second phase of this assault is more challenging to spot than the black hole attack. The Gray Hole Attack may be used in a number of ways, including by promoting a fictitious route, stealing device communications, and altering network state. The flow of data can be impacted by a variety of network issues. One is when certain nodes lose packets, which results in communication delays or even loss for other nodes. Another issue arises when a node acts maliciously and begins randomly dropping packets for a while before reverting to normal behavior later on. Even if you spot this sort of grey hole, it could be challenging to understand what it really wants or intends.

4.1.4 Byzantine Attacks

By operating alone or by causing packets to take unusual and unexpected courses, a hacked intermediate node, or a group of them working together, might interfere with the regular operation of routing systems. This can result in difficulties like loops, which send packets via the same route again; forwarding problems, which transport messages excessively far; or packet dropouts, which deteriorate the quality of communication.

4.1.5 Rushing Attack

How is it possible for assaults to rush? Attackers can stop the route discovery process in its tracks by bombarding nodes with packets before they have a chance to respond. Because on-demand routing protocols that employ duplication suppression rely on routers exchanging information about available routes to determine which way should be followed, these methods are the target of this attack. This trick prevents other routers from figuring out what pathways are available and how to best deploy them because invader nodes transmit all of their RREQ packets at once.

4.1.6 Link Spoofing Attack

In order to make it seem as though the malicious node is one of its one-hop neighbors, malicious nodes might include fictitious information into Hello messages. This strategy might be applied to make other nodes think that the malicious node has accurate information about them, thereby opening the way for attacks or data theft.

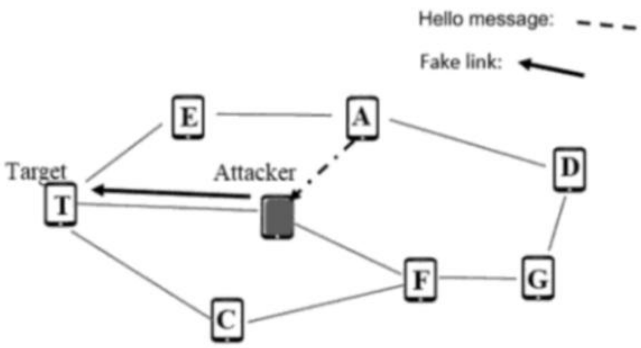

Figure 3: Link spoofing attack

4.1.7 Sybil Attack

A malicious node makes itself by manufacturing several nodes as opposed to the conventional one. Attacking other nodes or creating false identities for others are two methods to do this. A number of extra nodes, referred to as "Sybil" nodes, are also given false identifications by Sybil attackers. They do this to have an advantage over other competitors or to steal someone else's identity. These behaviours can prevent the correct resource allocation among the networked users, interfere with the operation of the routing protocol, and make it challenging to spot malicious conduct.

4.1.8 Flooding attacks

This attack's objective is to deplete a network's resources, including bandwidth, node computing power, and battery life. To make this happen, the attacker will make an effort to interact with the target system without any clear goal or intention. Performance suffers as a result of this resource wastage. Many of these resources are used up when trying to create routes for hypothetical locations that don't exist. An attack known as a route request flooding assault aims to overwhelm a network by sending a lot of packets (RRFA). The network becomes crowded and unable to transfer packets as a result of the excessive number of requests generated by this kind of attack.

4.1.9 Sink hole Attack

In this attack, the intruder tricks the neighbor nodes into believing that they are receiving proper routing information. This allows them access to other parts of the network and/or to alter data passing through it.

5 Conclusion

Mobile Ad hoc Networks (MANETs) are a less-configured infrastructure, which makes them more susceptible to security threats at different layers of the network protocol stack. Factors that contribute to MANET networks changing their topology and structure dynamically and without central oversight can lead to attacks or vulnerabilities being discovered in the system. In addition, cooperative algorithms used within MANETs make it difficult for defenders to identify an attack and take appropriate action.

In this paper, we will discuss the various ways in which an attacker can attack a networked system. We will provide a conceptual overview of detection mechanisms that are used to counteract these attacks, such as Black hole and wormhole attacks, sinkhole and flooding attacks, Link spoofing attacks, gray hole and rushing attacks. This paper should help readers understand how these different types of attackers operate or emerge at the network layer of MANETs.

References

[1]. David DS, S Deepa, Saxena GD, Singhal A, Bhalerao S. An Efficient Algorithm for Extricate Keywords in the text using High Utility Itemset Mining. Dongbei Daxue Xuebao/ Journal of Northeastern University. 2022;25(04):1754-73.

[2]. C Sharanya, Singhal A, S Balaji, Behera PC, Saxena GD, Dash C. Resourceful Decentralized Intellectual Routing Protocol For Wireless Sensor Networks. Dongbei Daxue Xuebao/ Journal of Northeastern University. 2022;25(04):1951–64.

[3]. Sharanya C, Gowtham MS, Jaya JA, Somasundaram K, S Balaji, Saxena GD, David DS. Development of Energy Competent Routing Protocol with Anfis Based Optimized Routing in Wireless Multi-Hop Ad Hoc Networks. Journal of Pharmaceutical Negative Results. 2022; 13(09): 5028-44.

[4]. Pathan AS, editor. Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC Press; 2016 Apr 19.

[5]. Pattnaik PK, Mall R. Fundamentals of Mobile Computing. PHI Learning Pvt. Ltd., 2015 Nov 30.

[6]. Yang H, Luo H, Ye F, Lu S, Zhang L. Security in mobile ad hoc networks: challenges and Solutions. IEEE wireless communications. 2004 Aug 16; 11(1): 38-47.

[7]. Kumar Singh U, Phuleria K, Sharma S, Goswami DN. An Analysis of Security Attacks found in Mobile Ad-hoc Network. International Journal of Advanced Research in Computer Science. 2014 May 1; 5(5).

[8]. Agal S, Dharmawat A. Security Issues in MANET: A review of Black hole Attack in MANET. International Journal of Computer Science & Technology. 2018.

[9]. Goyal P, Batra S, Singh A. A Literature review of Security attack in mobile ad-hoc network. International Journal of Computer Applications. 2010 Nov; 9(12): 11-5.

[10]. Sharma S. A Review of Vulnerabilities and attacks in Mobile Ad-hoc Networks. International Journal of Scientific Research in Network Security and Communication. 2018 Apr; 6(2): 66-9.

[11]. Jain A, Sawant K .Effect of Impersonation attack on mobile Ad hoc networks. Indian J Res. 2013 Mar; 2(3): 17-9.

[12]. El Bendru MA. Developing security tools of WSN and WBSN networks applications. Springer Japan; 2015 Jan 1.

[13]. Kumar V. A Fuzzy Based Control over Malicious Nodes in MANET. International Journal of Latest Trends in Engineering and Technology (IJLTET).

[14]. Bisen D, Sharma S. Fuzzy based detection of malicious activity for security assessment of MANET. National Academy science letters. 2018 Feb; 41(1): 23-8.

[15]. Simpson SV, Nagarajun G. A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment. Future Generation Computer Systems. 2021 Dec 1. 125: 544-63.

[16]. Dey R, Saha HN. Secure routing protocols for mobile ad hoc network (MANETs)- a review. Int. J. Emerg. Trends Techol. Comput. Sci. (IJETTCS). 2016 Feb; 5(1): 74-9.

[17]. Yadav H, Kumar P. Identification and removal of Black hole attack for Secure communication in MANET's. International Journal of Computer Scienceand Telecommunications. 2012 Sep; 3(9): 60-7.

[18]. Securing OLSR and STAR Routing Protocols.-IJCA online

[19]. Raza N, Umar Aftab M, Qasim Akbar M, Ashraf O, Irfan M. Mobile ad-hoc networks application and its challenges. Communications and Network. 2016; 8(03): 131-6.

[20]. Kaur V, Rani S. Prevention/ Detection Methods of Black Hole Attack: A Review. Advances in Wireless and Mobile Communications. Research India Publications. 2014: 10(4), pp. 747-56.

[21]. Mtenzi FJ, Oreku GS, Lupiana DM, Yonazi JJ, editors. Mobile technologies and socio economic development in emerging nations. IGI GLobal; 2018 Mar 23.

[22]. chlamtac I, Conti M, Liu JJ. obile ad hoc networking: imperatives and challenges. Ad hoc networks. 2003 Jul 1; 1(1): 13-64.

[23]. Veni RM, Latha R. Mobile ad hoc network. International Journal of Science and Research . 2013 Apr; 2(4).

[24]. Gupta R, Jain C. Mobile Ad hoc Network (MANETS): Proposed solution to Security Related Issues. Indian Journal of Computer Science and Engineering (ICSE). 2011 Oct; 2(5): 738-46.

[25]. AI-Omsari SA, Sumari P. An Overview of mobile ad hoc networks for the existing protocols and applications. arXiv preprint arXiv: 1003.3565. 2010 Mar 18.

[26]. Kumar R. Significance of Ad hoc networks: A review. International Journal of Computer Science & Communications. 2018; 9(1): 7-10.

[27]. Vinayakray-Jani P, Sanyal S. Routing protocols for mobile and vehicular Ad hoc networks: A Comprartive analysis. arXiv preprint arXiv: 1206.1918. 2012 Jun 9.

[28]. Abolhasan M, Wysocki T, Dutkiewicz E. A review of routing protocols for mobile ad hoc networks . 2004 Jan 1; 2(1): 1-22.

[29]. Chaturvedi K, Shrivastava K. Mobile Ad-hoc Network : A Review. International Journal of Innovative Research in Engineering and Multidisciplinary Physical Sciences. 2013: 1(1); 29-33.

[30]. Vanitha K, Rahman AM, Anitha K. An Analysis of Issues in Security and Routing Protocol in MANET. International Journal of Engineering REsearch & Technology (IERT), ISSN. 2014: 2278-0181.

[31]. Bhattacharya A, Banerjee A, Bose D, Saha HN, Bhattacharya D. Different Types of attacks in Mobile ADHOC networks. arXiv preprint arXiv: 1111.4090. 2011 Nov 17.

[32]. Nguyen HL, NGuyen UT. A study of different types of attacks in mobile ad hoc networks. In2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) 2012 Apr 29 (pp. 1-6). IEEE.

[33]. Panicker AV, Jisha G. Network Layer attacks and protection in ?MANET: A Survey. International Journal of Computer Science and Information Technologies. 2014; 5(3): 3437-43.

[34]. Rajkumar K, Prasanna C. Complete analysis of various attacks in MANET. Int. J. Pure Appl. Math. 2018; 119(15): 1721-7.

[35]. Gagandeep A, Kumar P. Analysis of different security attacks in MANETs on protocol stack A - review. International Journal of Engineering and Advanced Technology. 2012 Jun 5; 1(5): 269-75.

[36]. Seyyedataj M, Jamali MA. Different Types of attacks and detection techniques in mobile ad hoc networks. International Journal of Computer Applications Technology and Research. 2014; 3(9): 541-6.

[37]. Aluvala S, Sekhar KR, Vodnala D. An Emprical study of routing attacks in mobile ad hoc networks. Procedia Computer Science. 2016 Jan 1; 92:554-61.