International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 2, February 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Security Vulnerability and Counter Measures in Mobile Ad-Hoc Networks

Nwabueze, C. A[1]; Usiade, R. E[2]

[1]Department of Electrical/Electronic Engineering,
Chukwuemeka Odumegwu Ojukwu University Uli Anambra State, Uli, Nigeria
[2]Department of Computer Engineering, Delta State Polytechnic, Otefe-Oghara, Delta, Nigeria

ABSTRACT

The rising concern for beneficial, easy design and deployable, flexible, reliable, cost effective and scalable wireless network has led to the evolution of mobile Ad-hoc networks (MANETs). This type of network in its own peculiarity is a wireless, mobile, infrastructure-less network technology. It has been found to be very useful in military, commercial, personal, emergency related applications but not without some security challenges. The security of MANET is an important challenge to network engineers due to its unmonitored deployment nature and inherent resource limitation. This paper presents a study of some of these security issues that militate against ad hoc network technology design, deployment and operation. Possible counter measures required to overcome these challenges are also presented.

Keywords: MANET, Security, Attacks, Characteristics, Counter Measures

How to cite this paper: Nwabueze, C. A | Usiade, R. E "Security Vulnerability and Counter Measures in Mobile Ad-Hoc Networks" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-2, February 2020, pp.721-726, URL: www.ijtsrd.com/papers/ijtsrd30107.pdf

IJTSRD30107

1. INTRODUCTION:

Recent advancement in the field of information technology (IT) have given rise to many new applications. The wireless network technology is a driving force in this new application. This modern technology in IT advancement has been possible, innovative and beneficial considering the growth and acceptance of mobile wireless communication technology in recent time. Mobile wireless network technology can be classified into infrastructure and infrastructure less wireless network. The infrastructure wireless network is a network where the nodes (communicating devices) are connected with the fixed physical representation also known as Access Point (Helen and Arivazhagan, 2014). Figure 1 shows infrastructure (a) and infrastructure-less (b) networks.

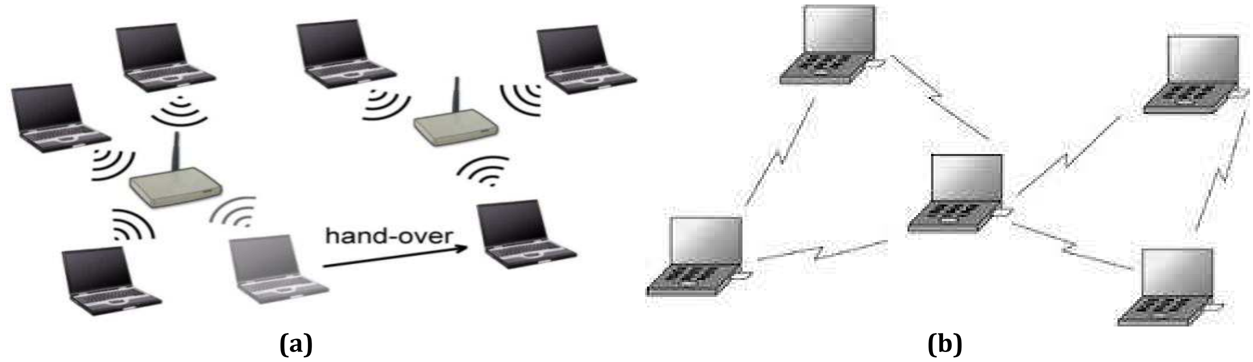

Figure1: Infrastructure and Infrastructure-less Wireless Networks.

The infrastructure-less wireless network is also known as a mobile Ad-hoc network. There are different descriptions adopted for this type of wireless network, however, the fundamental features remain the same.

According to Cason et al (1996), it is an autonomous system node connected with wireless link. Singh and Dhiman 2013, describe mobile Ad-hoc network (MANET) as a complex distributed system that comprises of wireless mobile node that are freely and dynamically self-organize into arbitrary and temporary network topologies.

Nithya et al 2016, described a mobile Ad hoc network as a collection of wireless nodes that can dynamically be set up anywhere, anytime without having the pre-existing network infrastructure. It is an autonomous collection of mobile devices which forms a temporary network without the aid of centralized administration or standard support devices regularly available in conventional networks. These different definitions of mobile Ad-hoc network outline some basic fundamental features/characteristics that are associated with this technology.

Some are highlighted as follows:
Autonomous Behavior: In mobile Ad-hoc network, each mobile terminal is an autonomous node. It simply means that each node in the network behaves both as host and router. Hence, besides is normal function as a node, it can also function as a switching device (router).

Distributed Operation: The mobile Ad-hoc network do not have any central control operational mode. In other words, the control and management of the network is distributed among the nodes. The nodes collaborate with each other to provide efficient routing protocol and handle their peculiar security issues.

Multi-Hop Routing: Mobile Ad-hoc network employ the principles of single hop transmission for nodes within the network transmission range. However, for transmission of data packets outside/beyond the transmission range, the network makes use of multi-hop transmission. Data packet delivery from a source to its destination beyond transmission range is forwarded through one or more intermediate nodes (Singh and Dhiman, 2013).

Dynamic Topology: The mobility feature of MANET makes it impossible to have a consistent topology. The configuration of the node keeps changing due to the mobile nature of the node. This consequently leads to changes in the routing table of the network.

Weak Link/Connectivity: Mobile Ad-hoc network makes use of wireless communication link. In this regard, the robustness, reliability, efficiency of its wireless links are often weaker/inferior when compared with wired links. This limitation makes them more prone to bit transmission error and security issues.

Similar Terminal Feature: All terminals in Mobile Ad-hoc network sometimes possess identical features with similar responsibilities and capabilities.

Network Scalability: The ease for Mobile Ad-hoc network configuration creates room for its expansion and upgrade. In some applications (large environment sensor, fabrics, battlefield deployment, urban vehicle grids) Mobile Ad-hoc network can grow to numerous thousand nodes (Kopekar and Kumar, 2015).

Terminal Energy Constraint: Mobile Ad-hoc network terminal devices have restrictions on the power source in order to maintain portability, size and weight (Aarti and Tyagis, 2013). They also possess less CPU (central processing unit) processing capability, smaller memory size. These limitations necessitate the need for algorithms which are energy efficient as well as operating with limited processing and memory resources.

Limited Bandwidth: Wireless link are known to have significantly lower capacity than infrastructure networks. In addition the efficiency of wireless communication medium have been found to be less when compared to wired medium due to the effect of multiple access, fading, noise, interference conditions, etc.

2. Mobile Ad Hoc Network (MANET) Security Criteria

Some of the features of MANET make it susceptible to security related challenges. The criteria used to determine and evaluate the security of MANET are as follows:
Authorization: This criterion assigns the different access right to different users (nodes) in the network.

Availability: The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of its security state (Mishra and Nadkarni, 2003). This criterion ensures that the node maintains its ability to provide all the designed services irrespective of the network operational status and the security measures adopted. It ensures the survivability of the network services despite denial of service attack.

Authentication: It ascertains the credibility of the network user. This ensures that participants in the network are genuine and they are not impersonators or imposters. Singh and Dhiman 2013, states that if there is no such authentication mechanism, the attacker could act as a benign node and thus get access to confidential information or even insert some false messages to disturb the normal network operations.

Uniqeness: This requirement ensures that malicious nodes do not resend previously captured data packets.

Confidentiality: Confidentiality means that certain information is only accessible to those who have been authorized to access it (Li and Joshi, 2008). It ensures vital information must be kept away from unauthorized users. According to Goyal et al, 2011, in order to maintain the confidentiality of some vital information, there is need to keep them secret from all entities that are not authorized and acknowledged to access them.

Integrity: Integrity guarantees the identity of the messages when they are transmitted. It ensures that data packets being transferred without are not corrupt. It also asserts that data are modified by authorized parties or in authorized way (Aarti and Tyagi, 2013).

Non-repudiation: It ensures the sender and receiver of the message cannot deny that they sent and received the massage (Gary and Mahapatra, 2009).

3. Security Attacks on MANET and Counter Measures

The need to secure mobile Ad-hoc network operation is very important. The absence of centralized monitoring and management system, absence of infrastructure, continuously changing (dynamic) topology and use of wireless transmission medium makes the network vulnerable to physical, digital and cyber security attacks. Some of these attacks can be in term of infiltration, eavesdropping, interference and so no. Security attack on MANET can be classified as either active attacks or passive attack:

The passive attacks are forms of attack which are difficult to identity. They do not disrupt the operation of the network but monitors its operation and violates the confidentiality criteria of the network. Examples include eavesdropping, traffic analysis.

The active attacks cause serious effects on the network operations. They are attacks that bear some energy cost in order to perform the attacks. In this form of attack, the intruder performs effective violation on either the network resources or data transmitted or both. Example is denial of service attack.

The various forms of attack on MANET and some possible counter measures include the following:

- **Impersonation**: It is a severe threat to MANET security. This form of attack allows the compromised node to join the network and perform malicious behavior like propagate fake data packets, alter the transmission of good/normal data packet. A good authentication measure can serve as an effective means for overcoming this form of attack.
- **Routing Table Corruption**: In this type of attack, the malicious node generates fake routing table or alters the configuration of the legitimate routing table or modify legitimate message from other nodes in order to add fake entire to the routing table. This attack can have non-optial routers, bottlenecks and even cause partitioning of certain parts of the network.
- **Denial of Service**: DoS attacks are aimed to complete disruption of routing information. The attackers flood the network with false routes and in addition disrupt the establishment of legal routes. Fellowship is a model based on obligation proposed in the direction of alleviating the packet flooding and dropping of packet in the network. Limitation rate of packets, restoration as well as enforcement are defined as the good constraints in this model (Balakrishnan et al, 2006).
- **Eavesdropping:** It means to obtain some confidential information that should be kept secret during communication. These information include public key, private key, location status, password of the nodes. Techniques of Frequency Hopping and Spread Spectrum Communication can protect the nodes from eavesdropping by preventing radio interface as shown in figure 2 (Hubaux et al, 2001).

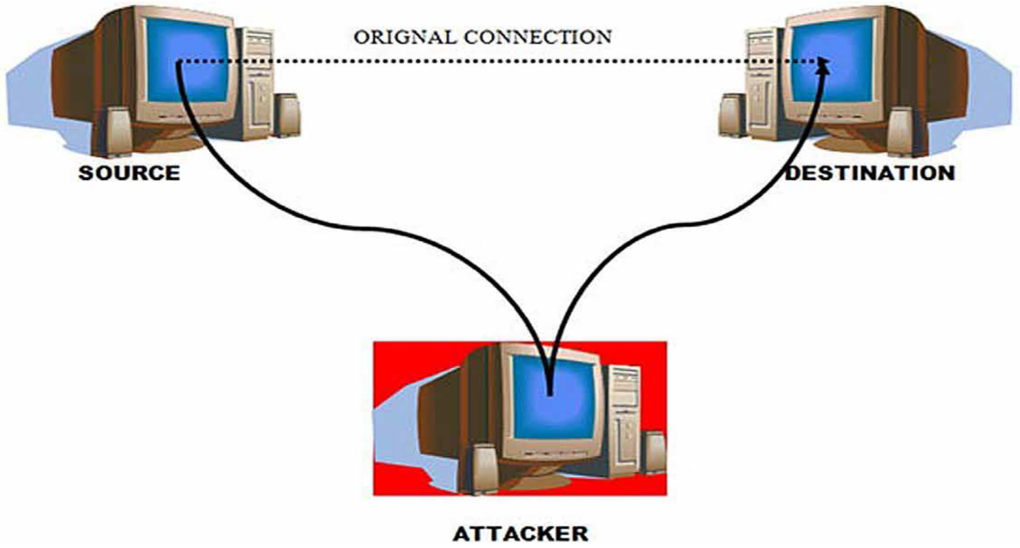

Figure2. Eavesdropping Attack in MANET (Hubaux et al, 2001).

- **Snooping:** This is unauthorized access to another person's node and includes the use of software program to remotely monitor activity on a terminal device. Good routing information can protect the network against this attack.
- **Location Disclosure:** It is a form of attack that targets the privacy requirement of a mobile Ad-hoc network.
- **Wormhole**: It involves cooperation of two malicious nodes. A node 'X' captures routing traffic at one point of the network to node 'Y'. Node 'Y' then injects the tunneled traffic back to the network. This type of attack is dangerous because it can cause damage to the network without any knowledge of such damage. According to Li and Joshi (2008), the use of packet leash is a general mechanism for detecting and, thus defending against wormhole attacks. A leash is any information that is

added to a packet designed to restrict the packet's maximum allowed transmission distance. There are two main leashes, which are geographical leashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed-of-light.

A geographical leash in conjunction with a signature scheme (a signature providing non repudiation), can be used to catch the attackers that pretend to reside at multiple locations (see figure 3).

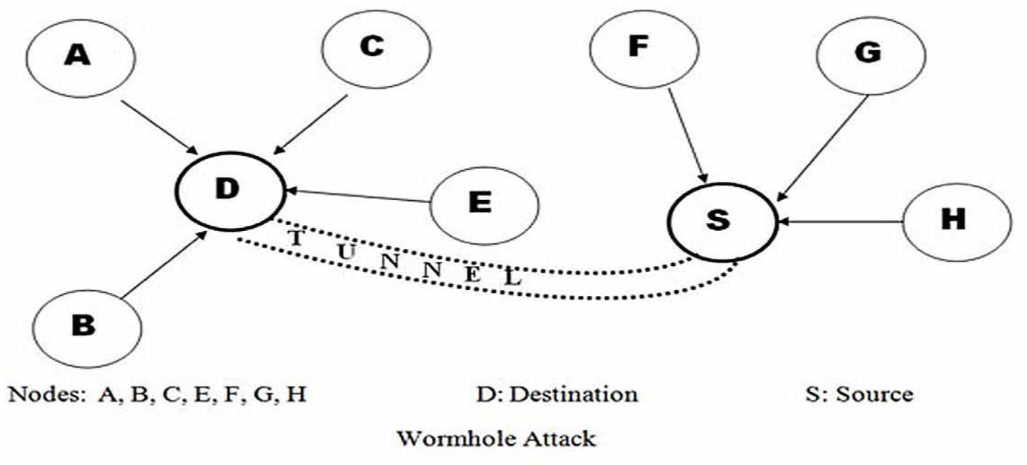

Figure3: Wormhole Attack in MANET (Li and Joshi, 2008)

- **Black hole**: In this attack, when a malicious node listen to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even itf no such route exists. As a result the malicious node easily misroute network traffic to it and then drop the packets transitory to it as depicted in figure 4 (Raja and Baboo, 2014). Khan and Islam (2012), presented a way to secure MANET against this form of attack. This can be achieved by using encryption and node location information. However, key distribution is a challenge in MANET.

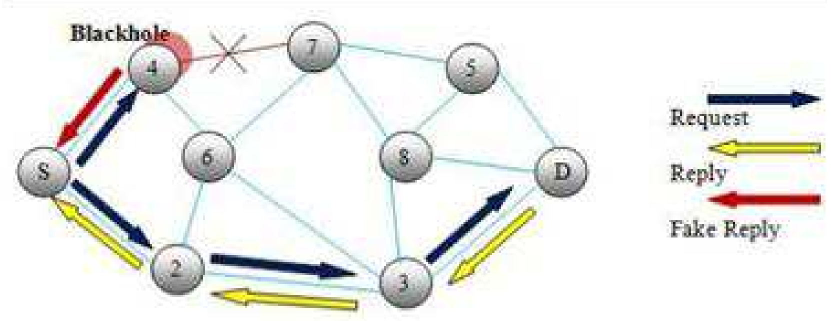

Figure4: Black hole Attack in MANET (Raja and Baboo, 2014).

- **Gray Hole Attack**: It is a form of route misbehavior attack which leads to dropping of messages.
- **Malicious Code Attack**: This is a type of virus attack which include; worms, spywares, Trojan horses which can attack both operating system and use application at the network terminal. A reliable anti-virus and other utility software applications can serve as good solution against these attacks.
- **Flooding Attack**: In this type of attack, the attacker exhausts the network resources such as bandwidth, battery power or disrupt the routing operation which causes degradation in network performance.
- **Traffic Monitoring and Analysis:** This type of attack involves the use of software to monitor the direction and frequency of traffic flow. Network topology, node location, mode of operation of the node, source and destination of data packets are some of the information this form of attack can expose. Monika and Rahul (2010) proposed that traffic analysis can be avoided by supporting link layer security and securing wireless MAC protocol.
- **Selfishness (Selfish Node Misbehavior):** Uncooperative act of node but distinct for evil behavior is referred to as selfish misbehavior. Such evil node makes use of the network resources only for selfish benefit and reject or refuse to send data packet from other nodes. They take unnecessary advantage of other nodes but do not allow their resources to be used.

  TWOACK is a very efficient scheme. It identifies the uncooperative behavior of nodes and explores to mitigate the cause through telling routing protocol (Kashyap et al, 2005).
- **Jamming:** In this form of attack, the attacker transmits data packet at the same speed/frequency with same two communicating nodes. This leads to conflict in the transmission link, between the two communicating parties. Regular forms of data packet (signed) jamming are random noise and pulse.

  Spread Spectrum Mechanism to block denial-of-service attacks could be a good solution.

- **Node Isolation Attack:** In this attack, the communicating nodes are isolated by not spreading communication link/medium to some particular collection of nodes or a node in the network. This keeps these set of nodes away from others in the network hence routing is not possible to these nodes (Kannhavong et al, 2006).

  This proposed counter measure is Intrusion Detection System (IDS), a local module of intrusion detection for OLSR. This module does non-conformance evaluation of each node in network and reveals the existence of attack on routing protocol.
- **Rushing attack**: In rushing attack, the compromised node receives a route request from the source node, it quickly floods the packet to other nodes in the network before the other node receive the some packet from the main source. This cause the other nodes upon the acknowledgment of the packet from the legal source, they will discard/reject it (see figure 5).

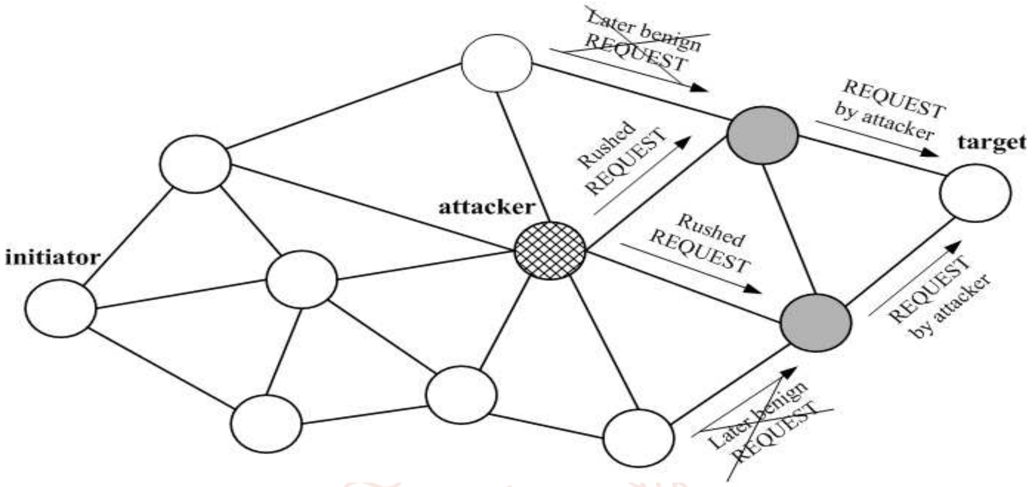

Figure5: Rushing Attack in Ad Hoc Network (Li and Joshi, 2008)

This attack can be overcome via a set of generic mechanisms that together defend against the rushing attack. These include *Secure Neighbor Detection*, *Secure Route Delegation*, and R*andomized Route Request Forwarding* (Li and Joshi, 2008). The relations among these security mechanisms are shown in figure 6.

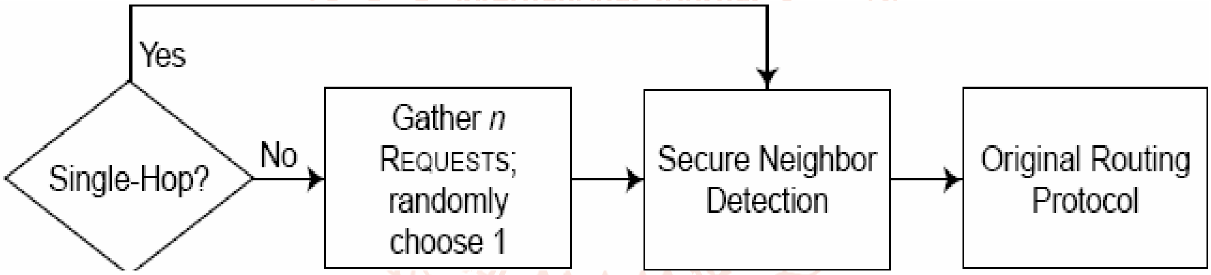
Yes
Single-Hop?
No
Gather n REQUESTS; randomly choose 1
Secure Neighbor Detection
Original Routing Protocol

Figure6: Combined Mechanisms to Secure MANET against Rushing Attacks (Li and Joshi, 2008)

- **Malicious Code attack**: This type of attack affects both operating systems and user application. A very good example include viruses, worms.
- **Session Hijacking:** The attacker exploits the unprotected session of its initial setup, spoofs the victim IP address, finds the correct sequence number and lunches various DoS attacks.

CONCLUSION

The security challenges of MANET is a very serious concern for both designers and operators. The reasons as clearly explained include resources limitation, dynamic topology, unmonitored deployment and lack of centralized management of the network due to the nature and reason of its configuration. This paper have contributed a lot in the measure of identifying some of these forms of attack and in addition proffer viable and resourceful counter measures and solutions. This work will assist mobile Ad hoc network designers and operators to take proactive measures to safeguard these resources and put up better performance during operations.

REFERENCES

[1] Aarti, F. and Tyagi, S. S. (2013), *Study of MANET: Characteristic, Challenges, Application and Security Attacks*, International Journal of Advanced Research in Computer Device and Software Engineering, Vol. 3, Issue 5, pp. 252 - 257.

[2] Balakrishnan, V., Varadharajan, V. and Tupakula U. K. (2006), *Fellowship: Defense Against Flooding and Packet Drop Attacks in MANET*, Network Operations and Management Symposium (NOMS 2006), pp. 1- 4.

[3] Corson, M. S., Batsee, S. and Maker, D. (1996), *Architected Consideration for Mobile Much Networking*, Proceedings of the IEEE Military Communication Conference (MILCOM), Vol. 1, pp. 225 – 229.

[4] Gary, N. and Mahapatra, R. P. (2009), *MANET Security Issues*, International Journal of Computer Science and Network Security, Vol. 9, No. 8.

[5] Goyal, P., Parmar, V. and Rishi, R. (2011), *MANET: Vulnerabilities, Challenges, Attacks, Application*, International Journal of Computational Engineering and Management, Vol.11.

[6] Helen, D. and Arivazhagan, D. (2014), *Application, Advantages and Challenges of Ad hoc Network*, Journal of Academic and Industrial Research. Vol. 2, Issue 8, pp. 453 – 457.

[7] Hubaux, J. P., Buttyan, L. and Capkun, S. (2001), *The Quest for Security in Mobile Ad Hoc Networks*, ACM Symposium on Mobile Ad hoc Networking and Computing.

[8] Kannhavong, B., Nakayama, H., Kata N., Nemoto, Y. and Jimalipoor, A. (2006), *Analysis of the Node Isolation Attack against OLSR Based Mobile Ad hoc Networking*, Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN 06), pp. 30 - 35.

[9] Kashyap Balakrishnan, Jing Deng, and Pramod K. Varshney, (2005), *TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks*, IEEE Conference on Ad Hoc Networks, 2005.

[10] Khan, Z. A. and Islam, M. H. (2012), *Wormhole Attack: A New Detection Technique*, International Conference on Emerging Technologies (ICET).

[11] Kopekor, S. and Kumer, A. (2015), *A Study of Ad hoc Wireless Network: Various Issues in Architecture and Protocols*, International Journal of Computer Applications, Vol. 12, No. 6, pp. 36 - 40.

[12] Li, W. and Joshi, A. (2008), *Security Issues in Mobile Ad Hoc Network - A Survey*, www.researchgate.net/publication/266280897.

[13] Mishra, A. and Nadkarni, K. M. (2003), *Security in Wireless Ad Hoc Networks*, The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, NY.

[14] Monika, M. K. and Rahul, R. (2010), *Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review*, International Journal of Computer Applications, Vol. 12, No.2.

[15] Nithya, S, Prema, S. and Sindho, G. (2016), *Security Issues and Challenges: Attributes In Mobile Ad hoc Networks*, International Research Journal of Engineering and Technology (IRJET), Vol. 3, Issue 01, pp. 1083-1087.

[16] Raja, L. and Babao, B. (2014), *An Overview of MANET: Application, Attacks and Challenges,* International Journal of Computer Science and Mobile Computing, Vol. 3, Issue 1, pp. 408-417.

[17] Singh, J. and Dhiman, N. (2013), *A Review Paper on Introduction to Mobile Ad hoc Network*, International Journal of Latest Trends on Engineering and Technology (IJLTET), Vol. 2, Issue 4, pp. 143-149.