# A Taxonomy of Physical Layer Attacks in MANET

Shefali Khatri
Department of CSE
Uttaranchal University
Dehradun

Punit Sharma
Department of CSE
Uttaranchal University
Dehradun

Prashant Chaudhary
Department of CSE
Uttaranchal University
Dehradun

Anchit Bijalwan
Department of CSE
Uttaranchal University
Dehradun

## ABSTRACT
In recent days, Mobile Adhoc Networks have emerged as a major next generation wireless network technology. The wireless and distributed nature of MANETs paves way for the intruder to degrade the functionality of MANET. MANETs are vulnerable to numerous attacks at all layers, because the design of most MANET routing protocols assumes as if there is no malicious intruder node in the network. MANET is a collection of self configurable mobile nodes where each node acts as a router for other nodes, which allows data to travel, utilizing multi-hop network paths. In this paper, we made an exhaustive survey on various attacks in MANET and we try to categorize various attacks on the physical layer.

## General terms
Mobile ad hoc network, Active attacks, Passive attacks

## Keywords
MANET, MAC, DSSS

## 1. INTRODUCTION
Present era is a "technological era". Technological revolution is an inevitable concept that has brought drastic changes in the concept of communication, networking, IT etc. Information technology is growing at an alarming rate day by day. Corporate sectors, businesses tend to use complex technological and network environments. MANET is one such variant for technological revolution which is in a strong pace to gain popularity as they provide wireless connectivity irrespective of their geographic position. Apart from this there are numerous other privileges provided by this adhoc networking that has acted as a boon in the field of networking.

Security is a crucial parameter that needs to be enforced in Mobile Ad-Hoc networking so as to ensure proper functioning of the network. Security in Mobile Ad-Hoc Network is of utmost importance. The success of MANET entirely depends on whether its security can be trusted and is reliable. However, the characteristics of MANET pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation.

One can achieve confidentiality, availability of network services and integrity of data only, when it is ensured that all the security issues have been met. Although various efforts have been laid down by the network administrators to secure the computing environments, still there exist some loopholes that act as a bridge for intruders to enter and destroy the data. There are several factors that pose threat to MANET because of its features like open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have paved way for the attackers to launch attacks and thereby disrupt normal functioning of the network. MANET is abbreviated term for "mobile ad hoc network". MANET is an infrastructure less network comprising mobile nodes that communicate with each other via wireless links and cooperate in a distributed manner so as to provide the necessary network functionality in the absence of a fixed infrastructure [1, 2].

MANET actually depicts an intricate form of distributed system that comprises wireless mobile nodes. These nodes have the liberty to organize themselves into arbitrary and temporary, ''ad-hoc'' network topologies, where people and devices can seamlessly interconnect with each other without requiring pre existing communication infrastructure. In case of mobile ad hoc network, nodes can directly communicate with all the other nodes within their proximity of radio ranges; whereas nodes that are not in the direct communication range are assisted by intermediate node(s) to communicate with each other. Figure 1 shows general description of MANET.

We categorized this research paper in four sections. In section 2 we study about the background details. Section 3 gives the classification of various attacks on MANET. In section 4 we have categorized various attacks on physical layer and discussed them along with their description.

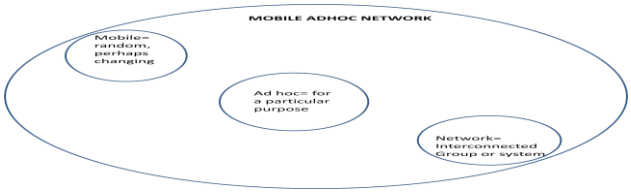


**Fig 1: General description of MANET**

## 2. BACKGROUND STUDY

Monika et al. [3], did exhaustive survey on security goals, security challenges and different types of active and passive attacks in MANET. She also explored some threatening vulnerabilities that occur due to features of mobile adhoc networks like dynamic topology, limited resources and zero central administration. Active and passive attacks corresponding to different layers are also discussed. C. Suhashini et al. [4], has proposed shift difference algorithm in order to transfer data securely over the network. She has also given detailed explanation regarding Triple Data Encryption Standard. Physical layer security has been provided by transmitting data as noise over the network. Murtaza A. Zafer et al. [5], considered the problem of channel reciprocity based secret key exchange over a wireless channel under an active jamming adversary. He further analyzed a broad class of information-theoretic secret key establishment protocols that are used to generate a secret key using common randomness, which can be obtained using the natural process of wireless fading. The paper basically focuses on secret key establishment phase of setting up the spread spectrum channel and thereby understanding limits and tradeoffs of this operation**.** K**.** Sivakumar et al**.** [6], in his paper have presented various key and trust management schemes to prevent against external attacks and secure routing protocols to defend against internal attacks in MANET. He also surveyed possible attacks in MANET that degrade the vulnerabilities in MANET along with their proactive and reactive solutions. He did exhaustive survey and presented two prevention techniques. First prevention technique is regarding secure routing and second regarding intrusion detection. J.G.Ponsam et al. [7] gave detailed explanation on various attacks concerning different layers. He further overviewed the challenges and gave possible solutions of the security threats in MANET. He summarized attacks along with its possible countermeasures to defend against them. V. Balakrishnan et al. [8], suggested three dimensions: cryptographic mechanisms, trust management and heterogeneous resource management to accomplish effective design of secure mobile wireless adhoc network. He also pointed on the issue that could threaten the security design which solely relies on cryptographic mechanisms. However, he suggested that the combination of trust management with cryptographic mechanism would help to cope up with such issues. To address the problem of divergence among nodes, the notion of heterogeneous resource management was also proposed by him. D.D. Aruna et al. [9], proposed a model that could be used as a countermeasure to cope up with signal jamming denial-of-service attacks in physical layer and network layer for MANET. In her model, she integrated SNAuth-SPMAODV (Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing) routing protocol with Direct Sequence Spread Spectrum (DSSS) which is a spread spectrum technology. Physical layer security is assured by this proposed methodology. Being a multipath protocol it assists in discovering multiple paths between sender and receiver without introducing extra packets into the network and it is also claimed to authenticate the neighbor. Dr.G.Padmavathi et al. [10], proposed a model that focuses on combining spread spectrum technology Direct Sequence Spread Spectrum (DSSS) with key management technique ISAKMP to cope up with signal jamming denial-of-service attacks in physical layer of MANET. (ISAKMP) ensures private communications on the Internet by combining the security concepts of key management, authentication, and security associations to establish the required security for private communications on the Internet.

## 3. NOXIOUS SECURITY ATTACKS ON MANET

An attack is an illegal attempt to modify, destroy, expose, alter or gain unauthorized access in order to disrupt normal flow of the system. MANET is more susceptible to security attacks as compared to traditional wired and wireless systems as the open nature of the wireless medium makes it easy for outsiders to listen to network traffic or interfere with it. Figure 2 shows graphical representation of various attacks corresponding to different layers in MANET.

### 3.1 Classification of Attacks

The MANET attacks can be classified based on different criteria like behavior, source of attack, their processing capacity and number of attackers involved. Table 1 shown below describes different attacks based on classification.

**Table 1. Attacks based on classification**

| Classification basis | Types | Brief description |
|---|---|---|
| Based on behavior | Active attack | **Active** causes instant modification. Aims at altering or destroying the resource. |
| | Passive attack | **A passive attack** aims only to steal the information. Do not cause any modification or fabrication. Very subtle and hard to detect. |
| Based on source (domain of attack) | Internal attack | **Internal attacks** carried out by malicious nodes that are part of network. |
| | External attack | **External attacks** carried out by nodes that do not belong to the network. |
| Based on processing capacity | Wired | **Wired**-intruders make use of wired medium to gain unauthorized access. |
| | Mobile | **Mobile**- intruders make use of wireless medium to gain unauthorized access. |
| Based on number of attackers involved | Single | **Single**-only one malicious node or person capable of disrupting the normal flow of network. |
| | Multiple | **Multiple**- more than one malicious node colludes in order to disrupt the normal functioning of the system. |

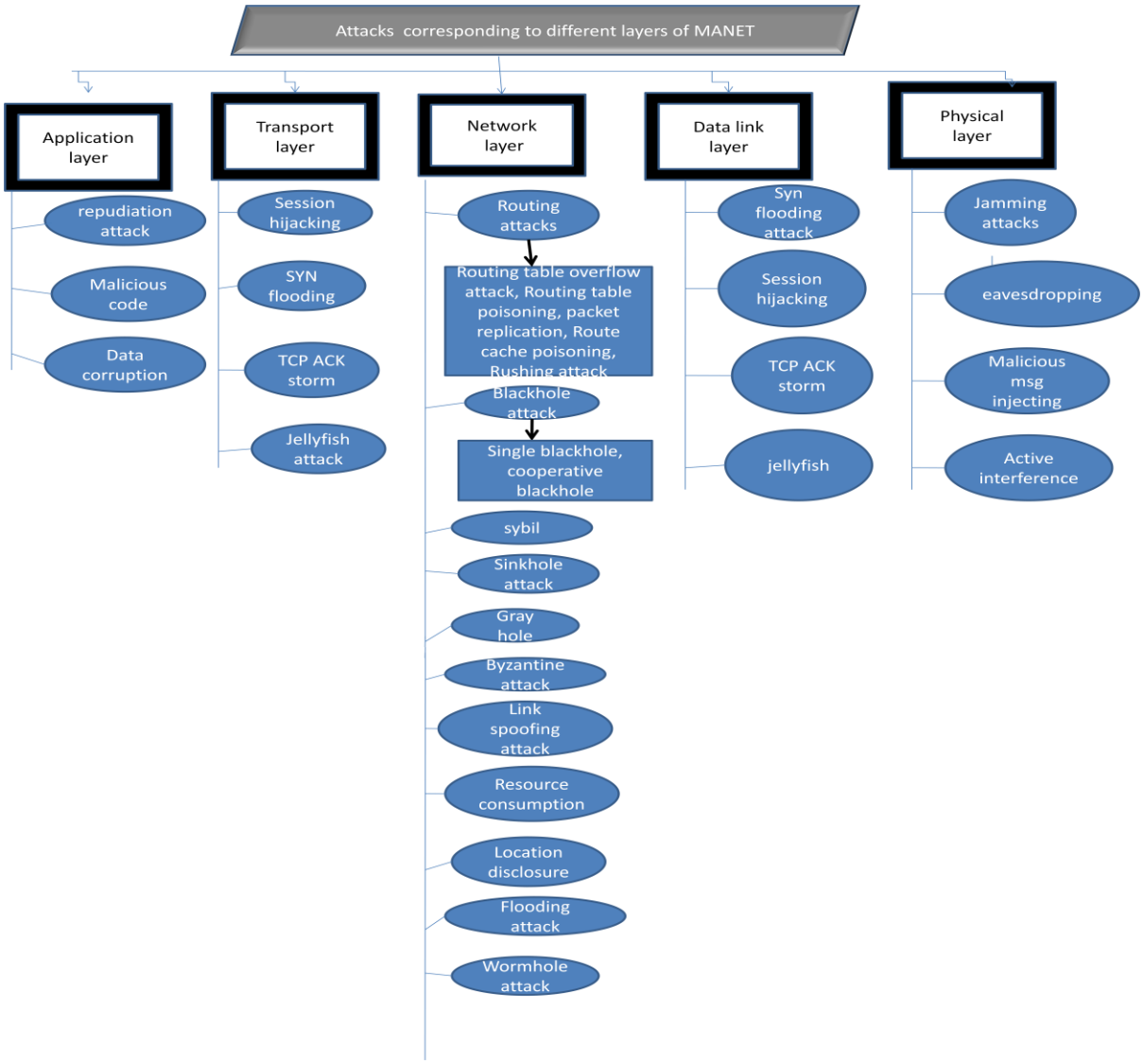


**Fig 2: Attacks corresponding to different layers in MANET**

## 4. ATTACKS CORRESPONDING TO PHYSICAL LAYER

Physical layer security is of utmost importance in MANET. The attacks on physical layer are basically hardware oriented and they only require little bit help from hardware sources to come into effect. Execution of these attacks is quite simple. They do not require the complete knowledge of technology. An attacker with sufficient transmission power and knowledge of the physical and medium access control layer mechanisms can easily gain access to the wireless medium. Here we will describe eavesdropping, interference, malicious message injecting and jamming attacks in brief. Figure 3 shows different attacks that target physical layer.

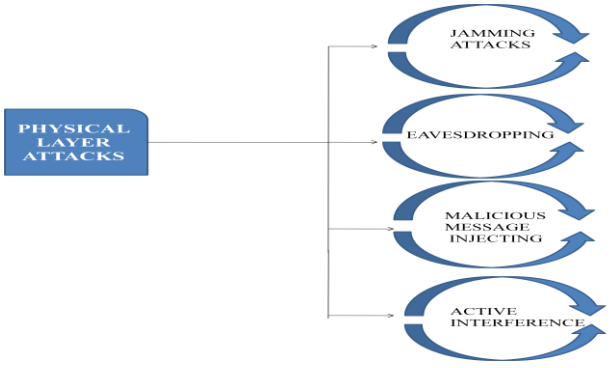


**Fig 3: Physical layer attacks**

## 4.1 Jamming Attack

A malicious or venomous node can continuously transmit a radio signal with the purpose to block any type of legitimate access to the medium or infer with the reception. This phenomenon is termed as jamming and the existing malicious node are termed as jammers. The messages can easily be corrupted by jamming or interfering with the Radio signals. A powerful transmitter is a vital tool that is required by the attacker to generate strong signal that has the potential to thrash the targeted signals and obstruct communications. Jamming attacks can be mounted from a remote location to the target networks. Signal jamming could be in the form of random noise and pulse.

Jamming is actually a type of DOS attack where malicious node aims at determining frequency of communication so as to launch this attack. Jammer along with the security threats transmits signals and thereby leads to prevention of legitimate packets [11]. There are different types of jamming attacks such as trivial jamming attacks, periodic jamming attacks and reactive jamming attacks as shown in figure 4. The brief descriptions of jamming attacks are provided in table 2 given below.

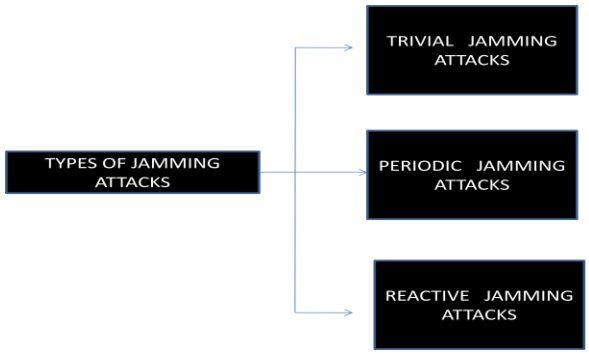


**Fig 4: Types of jamming attacks [12]**

**Table 2. Jamming Attack types**

| JAMMING ATTACK TYPES | DESCRIPTION OF ATTACK |
|---|---|
| TRIVIAL JAMMING ATTACK | Here an attacker transmits noise continuously over a period of time. All communications during this period are blocked. |
| PERIODIC JAMMING ATTACK | A short signal is periodically transmitted by the attacker. These transmissions can be further scheduled to hamper all other communications, also known as scrambling. |
| REACTIVE JAMMING ATTACK | A signal is transmitted by the attacker the moment he deduces that another node has initiated a transmission, leading to collision in other half i.e. second portion of the message. |

### *4.1.1 Jammers attack models*

Figure 5 represents different types of jammers along with their detailed explanation below.

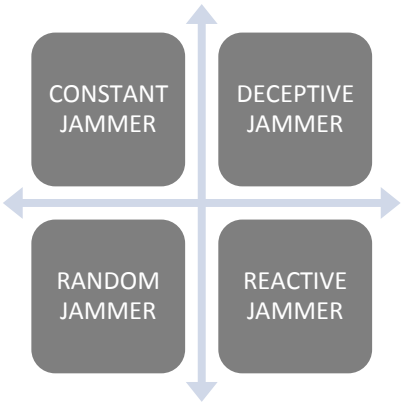


**Fig 5: Jammers**

#### *4.1.1.1 Constant jammer*

The constant jammer continuously emits random and useless radio signals. This jammer constantly sends out random bits to the channel ignoring any MAC layer etiquette. It does not wait for the channel to become idle before transmitting [13,14].

#### *4.1.1.2 Deceptive jammer*

It is responsible for injecting regular packets neglecting any sort of gap between subsequent packet transmissions.

#### *4.1.1.3 Random jammer*

This jammer alternates between sleeping and jamming. After jamming for tj units of time, it turns off its radio, and enters a sleeping mode. It will resume jamming after sleeping for ts time. Thus the jammer consecutively alternates between jamming and sleeping mode. tj and ts can be either random or fixed values. During its jamming phase, it can either behave like a constant jammer or a deceptive jammer.

#### *4.1.1.4 Reactive jammer*

It focuses on the point that it is not necessary to jam the channel when nobody is communicating. The jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. Consequently, a reactive jammer targets the reception of a message.

## 4.2 Eavesdropping Attack

Eavesdropping is an illegal attempt to monitor or intrude into other people's personal communications. Eavesdropper secretly listens the reliable conversation between two authentic parties.

Eavesdropping can be termed as intervening and reading of messages and conversations by unauthorized receivers [15,16]. The mobile hosts present in mobile ad hoc networks share a wireless medium. The majorities of wireless communications use the RF spectrum and broadcast by nature. As the communication takes place on wireless medium can easily be intercepted with receiver tuned to the proper frequency. In figure 6, the attacker keeps bird eye on procuring confidential information that is required to remain secret within the two authorized communicating parties. This confidential information may include private key, public key, location or passwords of the nodes. By

tapping communication lines, and wireless links it is easier to eavesdrop classified data.

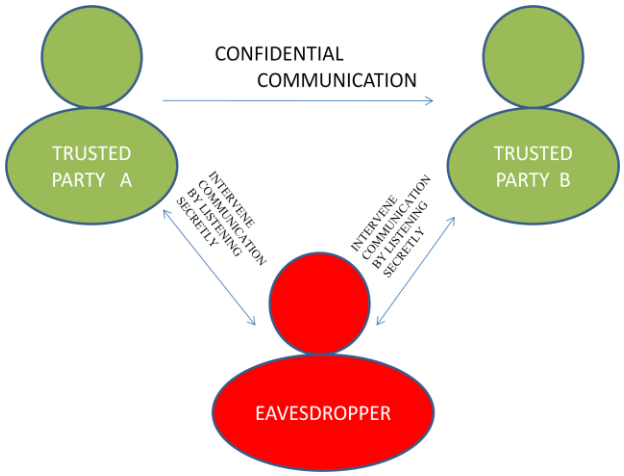


**Fig 6: Eavesdropping attack**

## 4.3 Malicious Message Injecting

Attacker injects false streams into the real message degrading the integrity of the message. Due to malicious message injecting the functionality of network is disrupted by the attacker. Figure 7 explains the overall process of malicious message injection.

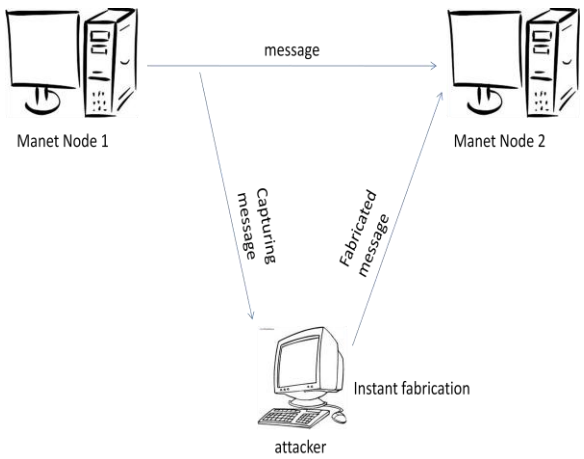


**Fig 7: Malicious Message Injecting**

## 4.4 Active Interference

It is a form of denial of service attack which blocks the wireless communication channel, or disrupts communications. The repercussion of such attacks depends on their duration, and the routing protocol [17,18]. Attacker will fabricate order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out of date information [19,11]. With respect to figure 8, MANET node 1 and MANET node 2 are involved in secret communication via messages but a malicious system will interrupt in between and will try to capture the message which is confidential. Further the attacker will try to modify the content of the message or replay it as a dos attack. MANET node 2 will actually receive a message which is no longer the original message but a fabricated one.

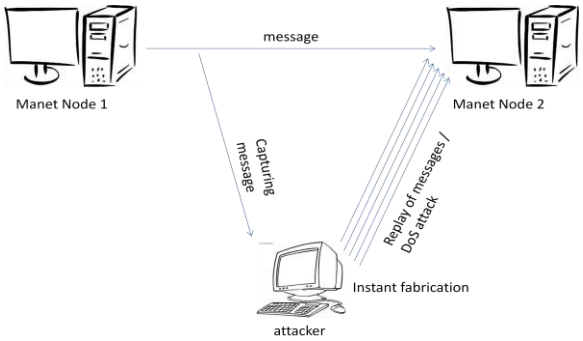


**Fig 8: Active Interference**

All the attacks mentioned above have been summarized in table 3 along with their countermeasures.

**Table 3. Attacks and their prevention**

| VENOMOUS ATTACK NAME | SHORT DESCRIPTION | COUNTERMEASURES TO COPE UP WITH |
|---|---|---|
| JAMMING ATTACK | Malicious node constantly transmit radio signals so as to block legitimate access | Packet Hiding Methods |
| EAVESDROPPING | Unauthorized intervention of the intruder where it listens secret information | Secure tunneling the channel data, encrypting the message. |
| MALICIOUS MESSAGE INJECTING | Injecting false streams into the real message hence degrading integrity of message. | Runtime execution monitoring by computing HMAC. |
| ACTIVE INTERFERENCE | Attacker fabricates order of messages or replay old messages. | Encryption , digital signature |

## 5. CONCLUSION

Security is an important aspect in MANETs. This paper has outlined various attack on MANET and made an exhaustive study of different attacks associated with physical layer against MANET and briefly described them in detail. Although MANET attacks can be prevented using different measures but prevention alone is not sufficient to deal with MANET attacks. Researchers should focus on enhancing existing techniques and generating new tools and techniques to tackle these attacks. In future,

emphasis should be laid on exploring techniques and algorithms that could cope up with physical layer attacks**.**

## 6. REFERENCES

[1] V.K.Upadhyay and R.Shukla, "An Assessment of Worm Hole attack over mobile ad-hoc Network as derious threats ", Int J. advanced Networking and Applications , Vol.5, Issue 1, ISSN : 0975-0290, August 2013.

[2] J.Thalor and Monika, "Wormhole attack detection and prevention technique in Mobile Adhoc Networks" ,International Journal of Advanced Research in computer Science and Software Engineering, Vol.3, Issue 2, February 2013.

[3] Monika, M.kumar and R.rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review", International Journal of Computer Applications (0975 – 8887), Volume 12– No.2, November 2010

[4] C.Suhashini and S. Sivakumar, "A Secure Approach with Physical Layer Encryption in MANET", International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 1, ISSN (Online) : 2319 – 8753, February 2014

[5] M.A.Zafer, D. Agrawal, and M.Srivatsa, "Bootstrapping Coalition MANETs: Physical-Layer Security under Active Adversary"

[6] K. Sivakumar and Dr. G.Selvaraj,"Overview of various attacks in Manet and countermeasures for attacks", International Journal of Computer Science and Management Research, Vol 2 Issue 1, ISSN 2278-733X, January 2013

[7] J. G. Ponsam and Dr. R.Srinivasan, "A Survey on MANET Security Challenges, Attacks and its Countermeasures", International Journal of Emerging Trends & Technology in Computer Science, Volume 3, Issue 1, ISSN 2278-6856, January – February 2014

[8] V. Balakrishnan and V.Varadharajan, "Designing Secure Wireless Mobile Ad hoc Networks" Information and Networked System Security Research Group

[9] D.Devi Aruna and Dr.P.Subashini , "Securing Physical and network layer using SNAuth-SPMAODV with DSSS for Mobile adhoc networks in Military Scenario", International Journal of Electronics and Computer Science Engineering, V1N3-1840-1849, ISSN- 2277-1956

[10] Dr.G.Padmavathi, Dr.P.Subashini and Ms.D.Devi Aruna, "DSSS with ISAKMP Key Management Protocol to Secure Physical Layer for Mobile Adhoc Network", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012

[11] S. Boora and S. Ohri," A Survey of Layer Specific and Cryptographic Primitive attacks and their countermeasures in Manet's",International Journal of P2P Network Trends and Technology (IJPTT) –Vol.3 Issue4- May 2013

[12] Jeremy J. Blum, Andrew Neiswender, and Azim Eskandarian,"Denial of Service Attacks on Inter- Vehicle Communication Networks" in 11th IEEE conference on Intelligent Transportation Systems, 2008, pp 797-802

[13] Le Wang and A.M.Wyglinski, "A Combined Approach for Distinguishing Different Types of Jamming Attacks Against Wireless Networks"

[14] G.Jayanthi Lakshmi,S. Babu , B Lakshmana Rao, P Mohan and B Sunil Kumar," Jamming Attacks Prevenrion in Wireless sensor Networks Using Secure Packet Hiding Method" International Journal of Advanced Research in Computer and Communication Engineering,Vol. 2, Issue 9, ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021 September 2013

[15] Ms. P. K. Karmore and S. T. Bodkh, "A survey On Intrusion in adhoc networks and its detection Measures"‖, International Journal on Computer Science and Engineering (IJCSE).

[16] M.Wazid, R. Kumar Singh & R. H. Goudar," A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques", International Journal of Computer Applications, International Conference on Computer Communication and Networks CSI- COMNET-2011.

[17] Zubair Muhammad Fadlullah, Tarik Taleb, and Marcus Schöller, "Combating against Security Attacks against Mobile Ad Hoc Networks (MANETs)".

[18] Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey".

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