ISSN No. 0976-5697

Volume 3, No. 5, Sept-Oct 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Survey on a Secured Layered Architecture for the Mobile Ad Hoc Networks

Swati Rani*
Department of Computer Science and Engineering
Amity School of Engineering and Technology
Lucknow, India
E-mail: with_Swati@yahoo.com

Parul Yadav
Department of Computer Science and Engineering
Amity School of Engineering and Technology
Lucknow, India
E-mail: pyadav@lko.amity.edu

Abstract: Mobile ad hoc network is a group of nodes that communicate via wireless links in the absence of a fixed infrastructure. The features of MANETs itself pose a number of opportunities and challenges to achieve the security goals that are authenticity, integrity, confidentiality, non-repudiation and availability. Security is an essential component in achieving basic network functions such as packet forwarding, routing and network management. This factor makes security the foremost concern of mobile ad hoc networks. Once it is ensured, only then these networks will gain confidence in the eyes of the commoners.

The most effective way to obtain security is via a layered architecture. A layered architecture can provide such advantages as modularity, simplicity, flexibility, and standardization of protocols. Since the layers should be protected from the malicious attacks occurring due to the malicious nodes therefore these nodes must be identified and stopped from acting as authorized nodes or routers. The identification of these nodes is a tedious task since they portray themselves as valid nodes and does not provide any clue to recognize them. The malicious nodes are capable of providing false routing information and can drop some or all the data packets that pass through them.

This paper provides the necessity of a layered architecture for security along with the overview of the mobile ad hoc network classification, advantages and disadvantages, vulnerabilities, challenges, applications, security goals and issues, attacks taking place in various layers.

Keywords: Malicious nodes, security, layered architecture, routing, data packets.

I. INTRODUCTION

An interconnected system of independent mobile devices may be configured as an autonomous network. These mobile devices then can communicate with each other over wireless links while functioning in a distributed manner. Such a networking with guaranteed interconnectivity is required in the absence of permanent infrastructures. Thus this configuration of a network can operate as a stand-alone network. The connectivity to the internet or other such networks may be achieved either at a single point or at multiple points. This type of networking connectivity makes it possible to open up various other options.

The mobile ad hoc network is decentralized. This also allows MANETs to use multi hop approach to deliver data. Since the nodes communicate over wireless links, they have to contend with the effects of radio communication, such as noise, fading, and interference [1]. Here the end users devices behave as both hosts and routers. The nodes can enter and leave over time. The data packets are forwarded by their immediate nodes to their final destination. In other words, network organization and message delivery is executed by the nodes that is to say that the routing functionality will be incorporated by the nodes themselves. Thus they are said to be self-organizing and adaptive.

One of the expected functionality of the devices in the mobile ad hoc network is that they should be able to detect the presence of other devices so that they can perform the necessary set up in order to facilitate communication and sharing of data and service. The devices can be easily added and removed to and from the network resulting in rapid change of the network topology which is fast and becomes unpredictable over time.

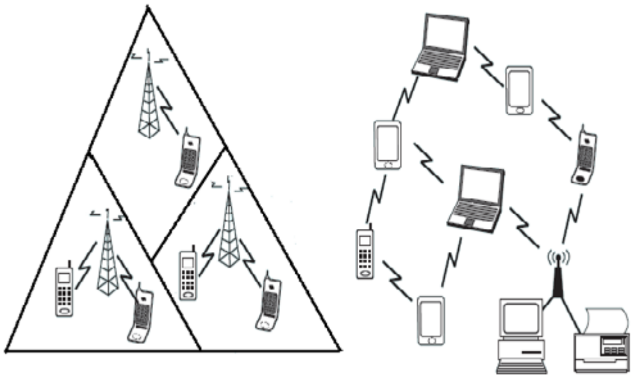

Figure 1: Cellular Network and Mobile Ad Hoc Network

The above diagram depicts a visual difference between the cellular network and the mobile ad hoc network. In case of the cellular network all the devices are connected to each other via base stations while in case of the mobile ad hoc network the mobile devices such as laptops, PDAs and phones communicate over wireless links. In other words, in the ad hoc networks, mobile nodes within each other's radio range communicate directly via wireless link using a protocol such as IEEE 802.11 [2] or Bluetooth [2], while those far apart rely on other nodes to relay messages as routers.

© 2010, IJARCS All Rights Reserved

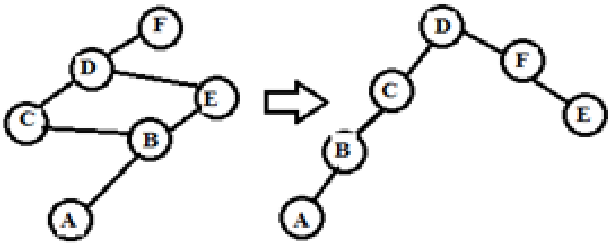

Figure 2: Topology Changes in the Mobile Ad Hoc Network

The first sequence of nodes shows the original network topology where node E is inside node B's radio range; therefore node B has a direct link with node E. When node E moves out of B's radio range, as shown in the second sequence of nodes, the original direct link between B and E is broken. However, the link from B to E is still kept, because B can reach E through C, D, and F [1].

It is essential to understand as to why a secured layered architecture is required for the mobile ad hoc network. The foundation on which this architecture will be constructed is explained hence forth. Some of the factors that are responsible can be mentioned as the vulnerabilities, challenges, applications, security goals and finally the attacks that are responsible for the existence of the various security mechanisms. The layered architecture will handle all the layers simultaneously thereby providing security against various existing attacks.

This paper is divided into seven sections. Section II contains a brief summary on MANETs which is further divided into sub sections containing the classification, advantages and disadvantages, etc. Section III provides a concept of layered architecture security. Section IV further specifies the various attacks occurring in the different layers. Section V contains the conclusion obtained from this paper and Section VII contains the future work that can be done for the security of the mobile ad hoc network. Section VII consists of the acknowledgement i.e. the people who helped me during the creation of this paper.

II. A BRIEF SUMMARY ON MANETs

Mobile Ad hoc Networks (MANETs) does not require any networking infrastructure in the form of base stations thereby allowing the devices to be absent from each other’s communication range in order to communicate. There are various types of MANETs. In spite of the vulnerabilities, disadvantages and challenges from which MANETs suffers; there are various advantages and applications in different areas of them. These can be summarized below:

A. Classification Of MANETs

MANETs can be classified as Vehicular Ad-Hoc Network (VANETs) which provide communication between the vehicles and the roadside equipment, Intelligent Vehicular Ad-Hoc Networks (InVANETs) which uses artificial intelligence and enables the vehicles to enact intelligently and thus helps in detecting the possible conditions and avoiding the vehicle collisions, accidents and even drunken driving, and lastly as Internet Based Mobile Ad-Hoc Network (iMANETs) that helps in connecting the mobile nodes and the fixed internet gateway nodes.

MANETs can also be roughly grouped as pure general purpose MANETs and other specified MANETs which further includes mesh networks, opportunistic networks, vehicular ad hoc networks and wireless networks [3]. The pure general purpose MANETs are used in battlefield and disaster recovery networks. Mesh Networks consists of both fixed and mobile nodes referred to as mesh routers that are connected to each other via wireless links and they construct a multi hop ad hoc network. Opportunistic networks can provide intermittent Internet connectivity to rural and developing areas where they typically represent the only affordable way to help bridging the digital divide as for wildlife monitoring [3]. VANETs provide efficient information regarding premonitions, emergency notifications and warning about traffic conditions.

B. Advantages And Disadvantages Of MANETs

There are various advantages and disadvantages of MANETs such as they provide access to information and services regardless of the geographic position and can be set up at any place and at any time. They have limited resources and physical security. The bandwidth of mobile ad hoc network is less as compared the wired network. They lack authorization facilities. Its unpredictable changing topology makes it hard to detect the malicious nodes. It requires a different set of security protocols since the security protocols for wired network cannot be used for mobile ad hoc network.

C. MANETs Applications

MANETs has diverse applications ranging from large scale mobile highly dynamic networks to small static networks. Typical applications include [4] [5]:

Military Battlefield: MANETs help in maintaining an information network between the soldiers, vehicles and military information headquarters.

Commercial Sector: MANETs are used in emergency and rescue operations to provide the disaster relief efforts mostly in cases of fire, flood and earthquake. Here the infrastructure based networks are not feasible since they can be damaged because of the calamity. And if one is depending on them then they can restrict the rescue operations from being performed. MANETs can also be used for enabling communication between the ships and law enforcement.

Local Level: MANETs help in linking the instant and temporary multimedia network like notebook computers or palmtop computers in order to facilitate sharing of information among the users at a conference or a classroom level. They can also be used in home networks where the devices communicate directly for sharing information. MANETs also find use in many other environments like taxicab, sports stadium, boat and small aircrafts [6].

Personal Area Network (PAN): Short-range MANET establishes intercommunication between various mobile devices such as a PDA, a laptop, and a cellular phone. MANETs help in replacing the tedious wired cables with wireless connections. An ad hoc network can also be extended to access the Internet or other networks with the help of Wireless LAN (WLAN), GPRS, and UMTS [7].

MANET-VoVoN: Using MANET-JXTA [8], a peer-to-peer, modular, open platform i.e. used to support user location and audio streaming, a client can search asynchronously for a user and a call setup until a path is available to reach the user. The application uses a private signaling protocol based on the exchange of XML messages over MANET-JXTA communication channels [8].

D. MANETs Vulnerabilities

Weaknesses in security system are termed as vulnerabilities. MANETs is more vulnerable than wired network. Some of them are:

Lack of centralized management makes it difficult for the nodes of the network to detect the attacks since it is not easy to monitor the traffic in a highly dynamic and large scale ad-hoc network.

Resource Availability includes the various security schemes and architectures play an important issue in providing secure communication.

Scalability of ad-hoc networks changes all the time unlike the wired network where it is predefined and does not change with use. This makes it difficult to keep a count of the nodes participating in communication or forming a network. Even the routing protocol and the key management service [9] have to comply with the occurring changes. Thus the security mechanism should be such that it is capable of handling large as well as small networks.

Cooperativeness is often taken for granted for the nodes for the routing algorithms since it is a necessity that should be established between the nodes but it often results in making a malicious attacker an important routing agent. Thus it will disrupt network operation.

Dynamic Topology disturbs the relationship among nodes and also affects the security of the network since this feature provides an opportunity to the malicious nodes to become a part of the network without being detected.

Limited Power Supply forces the nodes to behave in a selfish manner since the nodes of the mobile ad hoc network reply on battery as their power supply method [9]. Limited power supply gives rise to many problems. Each node of the network intends that the power is utilized by it only.

No Predefined Boundary enables even the malicious nodes to join and leave the network. Since there is no centralized entity that will keep a check of the nodes entering and leaving the network so this provides liberty to the attackers to become a valid part of the network and affect the network without being recognized. These nodes guarantee to provide the shortest path to the destination and when the data or information is passed then they drop some or all the data packets.

Adversary inside the Network exists due to one of the properties of MANETs itself which makes it hard to detect whether the node is malicious or not. Thus this attack is more dangerous than the external attacks since it is an extremely difficult job to identify the non valid nodes as they become an integral part of the network and behave like other nodes. So, one cannot differentiate between the authorized nodes and the malicious nodes.

E. MANETs Challenges

The characteristics of MANETs enforce many challenges on various layers. For instance the physical layer deals with rapid changes in the link characteristics. The media access control (MAC) allows fair channel access, minimizes packet collisions and deals with hidden and exposed terminals. The network layer enables the nodes to co-operate in order to calculate the paths. The transport handles packet loss and delay characteristics. The application layer handles the possible connections and reconnections [10].

Routing of packets between nodes is a challenging issue since the topology of the network constantly changes. Therefore is suggested that reactive approach should be used instead of proactive approach. MANETs uses multi hop approach to deliver data so the routes formed are complex as compared to the single hop approach.

Security and Reliability problems arise due to many reasons such as foul neighbor relaying packets. The wireless link characteristics such as the limited wireless transmission range, broadcast nature of the wireless medium also introduce the reliability problems. MANETs distributed nature requires authentication and key management.

Quality of Service (QoS) is an important concern since many factors affect it. This ensures that the information is being conveyed to an authorized node using a valid path. That is to say it does not contain any malicious node which will result in the loss of the data packets.

Inter-Networking between MANETs and fixed networks such as IP based is expected. Thus the existence of routing protocols for the same becomes a challenge since the routing protocols used for wired network are different than the ones used for the mobile ad hoc network.

Power Consumption should be low since it has a limited supply of power so if the consumption is not low then the nodes are forced to behave in a selfish manner.

Multicast is desirable to support multiparty wireless communication. Since the multicast tree is no longer static, the multicast routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join) [7].

Location Aided Routing uses positioning information to define associated regions so that the routing is spatially oriented and limited.

F. MANETs Security Goals

The security problems arises basically because of five reasons[11] that are open medium which makes eavesdropping easier in the mobile ad hoc network than the wired network, the dynamically changing network topology which provides an opportunity to the malicious nodes to become a part of the network, the co-operative feature required by the routing algorithms which builds the trust between the involved nodes but surpasses the security conditions, lack of centralized monitoring due to which the entire cannot be checked and controlled by the central entity and lack of a clear line of defense that implies that a single line of defense is not sufficient for attack prevention thereby laying the basis for the requirement of the second line of defense which provides detection and response.

The security goals consist of the security grounds on which an analysis can be made to know whether a mobile ad hoc network is secure or not. Basically security goals provide the criteria that should be followed to produce a secure mobile ad hoc network. They can be enlisted as:

Availability aims at providing all the expected and required data and services by the assets or nodes at appropriate time to authorized parties regardless of the denial of service attack.

Integrity aims at securing the nodes to be accessed only by the authorized parties in an authorized way. These authorized parties can modify the contents. Creation, deletion, writing and status changing are the basic modifications. Integrity is affected by either by malicious altering or by accidental altering. A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering [9].

Confidentiality also referred to as secrecy or privacy ensures that the nodes or assets information is viewed only by the righteous holders i.e. the ones which actually have the right to do so. This information should be kept hidden from the false parties or the unauthorized parties.

Authentication helps in confirming the identity of the communicating node. The nodes can check themselves whether the node to which they are communicating are valid or not with the help of the encrypted message sent by the sender that will be decrypted only by the shared key. Thus it ensures whether a node is genuine or an impersonator.

Non Repudiation stops the nodes from denying that they have sent or received a message. This helps in identifying the malicious nodes. Since if a node denies then this indicates that is not a valid node and is sending false information to the other nodes of the network. Once identified, these can be treated for removal.

Authorization is like certificate authority that cannot be nullified and indicates the rights and functions held by the user. It provides a description of the access rights of different levels of users [9].

Anonymity consists of all the data that helps in identifying the current user of a particular node. This information is kept secret and not to be distributed.

G. ATTACKS IN MANETs

There are two types of attacks, namely

- **Internal Attacks** are casted by the compromised nodes within the network. These nodes are capable of accessing the protected rights of the network resulting in the collection of the security information.
- **External Attacks** are casted by the adversaries that do not belong to the network. They can further be classified as :

Passive Attacks detects the data exchanged in the network (called snooping) without disturbing the communication operation.
Active Attacks detects and destroys the data exchanged in the network thereby disturbing the communication operation. There are various types of active attacks.

The security attacks can be broadly divided into categories i.e. route logic compromise and traffic distortion attack [11]. The former includes the insertion of false routing control messages into the network with the intension of harming the routing information. The latter focuses on the non delivery of data packets from source to destination. The attackers gain the information carried, corrupt it, block the transmission or provide false reply.

III. LAYERED ARCHITECTURE

The security of the network cannot be considered after the whole infrastructure has been designed. In fact it should be taken into consideration and inculcated at each phase of its design. In other words it should not be added as a conclusion for each step rather it should be incorporated as an integral part of the step. Different architectures have been proposed by various researchers to ensure security [12] [13]. All these architectures work on the basis of the OSI model [14] [15]i.e. the open system interconnection model which deals with connecting open systems i.e. the systems that are open for communication with other systems.

© 2010, IJARCS All Rights Reserved

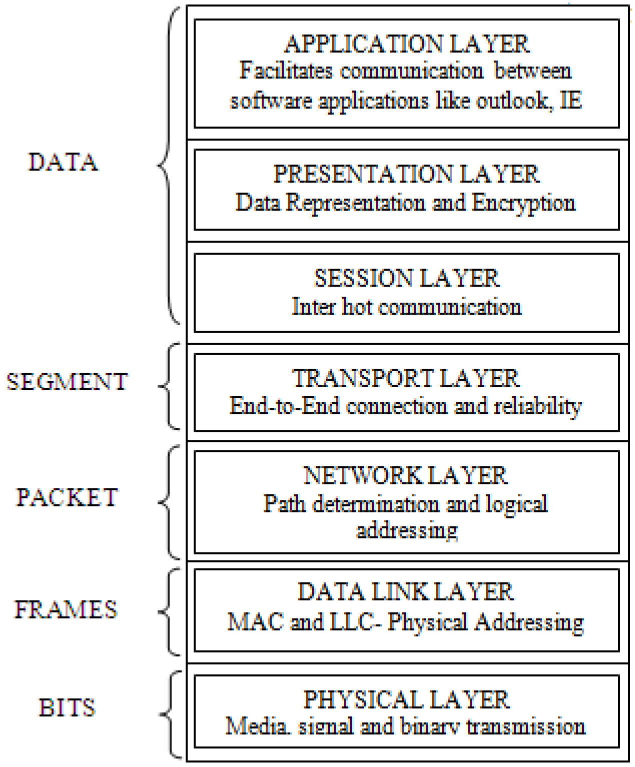
DATA
SEGMENT
PACKET
FRAMES
BITS
APPLICATION LAYER
Facilitates communication between software applications like outlook, IE
PRESENTATION LAYER
Data Representation and Encryption
SESSION LAYER
Inter hot communication
TRANSPORT LAYER
End-to-End connection and reliability
NETWORK LAYER
Path determination and logical addressing
DATA LINK LAYER
MAC and LLC- Physical Addressing
PHYSICAL LAYER
Media, signal and binary transmission

Figure 3: Different Layers of the OSI Model

The above figure describes the various layers of the OSI Model along with their functions and the form of the data they are carrying.

Various security attacks exist for different layers such as in physical layer jamming and eavesdropping take place. Black hole, grey hole, warm hole, information disclosure, message altering, sending data to node out, routing attacks take place in the network layer. Session hi-jacking takes place in transport layer while repudiation in application layer. Denial of service, impersonation, man in the middle attack takes place in the multi layer. Thus these layers provide certain security issues.

The application layer detects and prevents viruses, worms, malicious nodes and application abuses with the help of intrusion detection systems. The transport layer authenticates and secures end to end communication through data encryption. Network layer protects the ad-hoc routing and forwarding protocols. Link layer protects the wireless MAC protocol providing link layer security support. Physical layer prevents signal jamming and denial of service attack.

Since different layers have their own way of protection [16] [17] and all of these security protocols are designed for some specific security requirement and their overlapping functionalities make the whole system inefficient and complex and at times it becomes a big headache for users to choose and deploy. The existing architectures are basically concerned with establishing the trust infrastructure alone, or just concerns with securing routing protocol based on certain assumptions. None of them provide a solution from a system architectural view or describes the whole picture of how the building blocks of security mechanisms are combined together to fulfill the security requirement of MANETs. A layered architecture can provide such advantages as modularity, simplicity, flexibility, and standardization of protocols [18].

IV. ATTACKS IN EACH LAYER

Each layer has its own set of errors. A brief summary of the attacks of different layers is given as

A. *Physical Layer Attacks*

The physical layer co-ordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specification and defines the procedures and functions of the interface and the transmitting media. It also defines the type of the transmitting medium, the representation of bits and the duration of bits i.e. the data rate. It also helps in synchronizing the sender and the receiver clocks.

Eavesdropping and jamming mostly occur in this layer.

Eavesdropping (a passive attack) enables the malicious nodes to silently observe the confidential information and use it later. In other words the secret information being transmitted is preserved by the attackers and fake messages are injected into the network.

Jamming occurs when various data packets are transmitted accidently or intentionally at the same frequency. Jammers are of two types i.e. the high power pulsed full band jammers and the low power partial band jammers [19].

B. *Link Layer Attacks*

This layer helps in transforming the physical layer into a reliable link by making it error free for the upper layer. It divides the stream of bits received from network layer into manageable data units called frames to which a header a added defining the address of the sender and the receiver. It also performs flow control, error control and access control.

The link layer protocols are used to maintain the one hop connectivity among the neighbors therefore the attacks mainly focus on disturbing this cooperation.

C. *Network Layer Attacks*

This layer is responsible for the source to destination delivery of a packet across multiple networks [20]. Its major duties are logical addressing and routing [21].

This layer protocols extend connectivity from a hop to all other nodes in the network. Whenever an attacker attacks a routing protocol; it actually includes itself in the routing path and control the network traffic flow. This enables the packets to follow a non-optimal path and creates unnecessary delay. These attacks force the data packets to follow a non-existent path and thus get lost. They even create routing loops, network congestion and in severe cases may even prevent the data packets to at all find any path to the destination thereby decreasing the performance of the network.

© 2010, IJARCS All Rights Reserved

The attackers attack at the routing discovery phase, routing maintenance phase and data forwarding phase.

Wormhole attack, black hole, byzantine attack, rushing attack, resource consumption attack, location disclosure attack also occur in the network layer.

Routing Attacks take place because of the malicious nodes. These nodes create problem in the propagation path of the information. The attacks against routing can be classified into two categories i.e. attacks on the routing protocols and attacks on the packet forwarding/delivery [22]. The former focuses on disrupting the communication path while the latter focuses on disrupting the data packet that is being communicated.

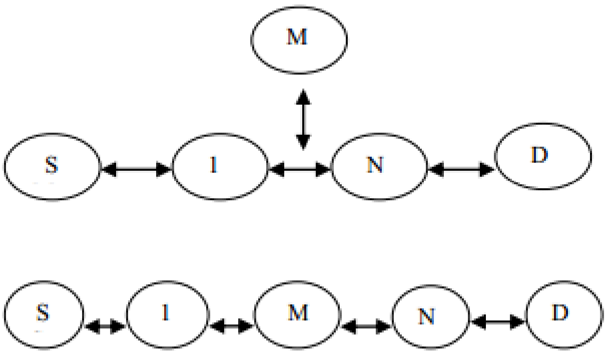

Figure 4. Malicious node becoming part of the network

In the Figure a malicious node M injects itself into the routing path between sender S and receiver D.

Black Hole Attacks creates an illusion of a zero metric for all destinations enabling the surrounding nodes to route their packet towards it. The malicious node portray that they have an optimum route and make the genuine nodes send their data packets towards it. These data packets are then dropped by the malicious nodes.

Wormhole Attack is a generalized form of repeater attack. It consists of two nodes that are connected to each other via a tunnel. Here the attacker records the data packet at one point in the network, tunnels it to another point or location in the network and replays the packet from the second location or point [20]. Tunneling is done either by using single long range directional wireless link or through a direct wired link [23].

Byzantine Attack takes place when a single or a set of compromised nodes works in collision and creates routing loops, forwards the packets through non-optimal paths, drops packets. Thus degrade the routing services.

Rushing Attack acts as an effective denial of service attack. Here the malicious act is desperate to become a part of the routing path. So when the source sends out RREQ then these malicious nodes rushes to respond to the source node with a valid response.

Resource Consumption Attack also referred to as the sleep deprivation attack consumes the battery life by requesting excessive route discovery or by forwarding unnecessary packets to the victim node.

Location Disclosure Attack publicizes the information regarding the location and structure of the node and then makes schemes for further attack.

Replay Attack retransmits the valid data repeatedly into the network path thereby increasing traffic in the path.

Gray Hole Attack is also known as the routing misbehavior attack and results in the dropping of messages. It takes place in two steps. First includes the false promotion of the malicious node as to have a valid route to the destination. And the second step consists of dropping the data packets either selectively or completely as they pass through them.

D. *Transport Layer Attacks*

This layer is responsible for the process to process delivery of the entire message. It ensures that the message arises intact and in order. Port addressing, segmentation and reassembly, connection control, flow control and error control form the responsibilities of the transport layer.

The transport layer protocols include setting up of end to end connection and end to end reliable delivery of packets, flow control, congestion control and clearing of end to end connection [24]. SYN flooding attack and session hijacking take place at the transport layer.

Session Hijacking utilizes the information that the communications are secured at session setup only and not afterwards.

SYN Flooding Attack is a denial of service attack. Due to this attack a large number of half opened TCP connections are opened with a victim node. It never completes the handshake.

E. *Application Layer Attacks*

This layer enables the user i.e. human or software to access the network by providing user interfaces and support for services such as the electronic mail, World Wide Web access, remote file access and transfer by creating a virtual terminal.

Mobile Viruses & worm attacks and repudiation attacks take place in the application layer.

Repudiation Attack occurs when a node's participation in any communication is denied that is to say that the nodes disclaim have sending or receiving a data packet.

Mobile Virus and Worm Attacks occur when the malicious nodes that contain these data are applied on the operating systems and applications.

F. *Multi-Layer Attacks*

There are certain attacks that are casted from multiple layers. They can be denial of service, impersonation attack and man in the middle attack [25].

Denial of Service Attack focuses on attacking the availability of the node or the entire network. Its success denies the services provided by the specific node or network.

© 2010, IJARCS All Rights Reserved

This attack is caused by the radio jamming signal and battery exhaustion.

Impersonation enables the malicious nodes to act as genuine node and thus access the confidential data. Since there is no central entity, the addition or deletion of nodes to the network is not checked. Thus the malicious nodes can be easily added to the network and thus affect the delivery of data packets from the source to the destination.

Man in the middle attack means that an attacker exists between a sender and a receiver and is detecting the exchanged information.

V. CONCLUSION

Mobile ad hoc network is thus a versatile way of communication which is spontaneous and highly flexible that is self-creating, self-organizing and self-administering wireless network. Its intrinsic adaptability to changing situations and demands, independent of permanent infrastructure, ease of deployment, auto-configuration, low cost and myriad applications makes it an essential part of future pervasive computing environments. This system of ad hoc communication is not free of challenges; it has large number of impediments that need to be addressed like protocols, applications, services and security.

There are various types of attack and their counter measures have been identified. Yet there are attacks that are unpredictable. In order to provide security to the various attacks taking place in the various layers; an introduction to the layered architecture has been provided. This method will help in providing a better security solution. This architecture provides an opportunity to increase the efficiency of the devices and technology in use.

VI. FUTURE WORK

This paper consists of all the basic information that will enable one to understand and get the answer to their question as to what is MANETs. All the vulnerabilities faced by it, the various challenges, applications and security goals and the various attacks have been enlisted. The concept of the layered architecture for providing security can be worked on by the users. The functions provided by the various layers and its practical implementation if of foremost importance. Further this model can be tested for the various MANETs applications and how it can be used to eliminate or reduce the various existing attacks.

VII. ACKNOWLEDGEMENTS

I am highly grateful to my teachers who helped me in clarifying my doubts and also my friends and classmates who were a real help.

VIII. REFERENCES

[1]. http://www.netlab.tkk.fi/opetus/s38030/k02/Papers/14-Zheng.pdf

[2]. T. Karygiannis and L. Owens, “Wireless Network Security-802.11, Bluetooth and Handheld Devices”. Special Publication 800-848, 2002

[3]. http://www.jiaziyi.com/documents/20080229_A_Survey_on_the_Applications_of_MANET.pdf

[4]. M. Frodigh, P. Johansson, and P. Larsson, "Wireless ad hoc networking: the art of networking without a network", Ericsson Review,No.4, 2000, pp. 248-263.

[5]. HaoYang, Haiyun & Fan Ye,"Security in mobile ad-hoc networks : Challenges and solutions", Vol 11, issue 1, Pg. 38-47, Feb 2004.

[6]. http://www.mediateam.oulu.fi/publications/pdf/92.pdf.

[7]. Priyanka Goyal, Vinti Parmar,Rahul Rish, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM, Vol. 11, January 2011, Pages 32-37.

[8]. Luis Bernardo, Rodolfo Oliveira, Sérgio Gaspar, David Paulino, and Paulo Pinto, “A Telephony Application For MANETs Voice Over A MANET-Extended JXTA Virtual Overlay Network”, Communications in Computer and Information Science Volume 9, 2008, pp 347-358.

[9]. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Applications and Challenges”, Journal of the Communications Network, Vol. 3 (July 2004), pp. 60-66.

[10]. http://www.cn.apan.net/cairns/NRW/43-Yu%20Shuyao.pdf

[11]. L.Buttyan, J. Hubaux,"Enforcing Service Availability in Mobile Ad-Hoc WANs", Proceedings MobiHoc '00 Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing, IEEE Press Piscataway, NJ, USA ©2000, ISBN:0-7803-6534-8, Pages 87 – 96.

[12]. L. Zhou and Z. Hass, “ Securing Ad Hoc Networks ” , IEEE network, vol 13, no.6 pp24 -30, 1999.

[13]. http://www.cs.ucla.edu/wing/publication/papers/Kong.ICNP01.pdf

[14]. S. Capkun, L. Buttyan, J. Hubaux:, "Self -Organized Public-Key Management for Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing archive, Volume 2 Issue 1, January-March 2003, Page 52-64.

[15]. Y. Zhang, W. Lee, "Intrusion Detection in Wireless Ad -Hoc Networks", Proceedings MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking, ACM New York, NY, USA ©2000, ISBN:1-58113-197-6, Pages 275-283.

[16]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks” , International Journal of Engineering Science and Technology , Vol. 2(9), 2010, Pages 4063-4071.

[17]. Wenjia Li and Anupam Joshi , “Security Issues in Mobile Ad Hoc Networks- A Survey” , The 17 th White House Papers Graduate Research In Informatics at Sussex, (2004), pp.1-23.

[18]. http://martinolivier.com/open/lasa.pdf

[19]. Tao Lin, “Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications” , Journal Of Information, Knowledge And Research In Computer Science And Applications, ISSN: 0975 – 6728, Nov 09 To Oct 10, Volume 1, Issue 1, Page 6-12.

[20]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions”, IEEE Wireless Communications, pp. 38-47, 2004.

[21]. G.S. Mamatha , “Network Layer Attacks and Defense Mechanisms in MANETS- A Survey” , International Journal of Computer Applications (0975 – 8887), Volume 9– No.9, November 2010, Pages 12-17.

[22]. Y. Xiao, X. Shen, and D.-Z. Du (Eds.),“Wireless/Mobile Network Security” , Proceeding ICCCS '11 Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM New York, NY, USA ©2011, ISBN: 978-1-4503-0464-1, Pages 114-118.

[23]. Y. Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing”, IEEE Security & Privacy, pp. 28-39, 2004.

© 2010, IJARCS All Rights Reserved

[24]. W. Lou and Y. Fang, “A Survey of Wireless Security in Mobile Ad Hoc Net-works: Challenges and Available Solutions. Ad Hoc Wireless Networks”, edited by X. Chen, X. Huang and D. Du. Kluwer Academic Publishers, pp. 319-364, 2003.

[25]. L. Zhou and Z. Haas, “Securing Ad Hoc Networks”, IEEE Network Magazine Vol.13 No.6 (1999) pp. 24-30.