ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

A Review on Layer Wise Security Issues and Possible Remedies in Mobile Ad hoc Networks

Mohammed Aziz Ahmed[1], Mohammed Sirajuddin[2], Nazia Kouser[3]

Research Scholar, Department of CSE, Shri Venkateshwara University, Gajraula, Amroha (UP) India [1]

Visiting Professor, Departments of CSE, Shri Venkateshwara University, Gajraula, Amroha (UP) India [2]

Research Scholar, Department of ECE, Shri Venkateshwara University, Gajraula, Amroha (UP) India [3]

ABSTRACT: There is no doubt many researchers have proposed several safe and secure routing layer design, but the resistance of those proposed and secure routing layer design towards various types of security attacks and efficiency are primary points of concern. In this paper we tried to concentrate on security issues and possible solutions layer wise.

KEYWORDS: Security Issues, Possible Remedies, MANET, Network Architecture, Network Topology,Protocols.

I. INTRODUCTION

An ad hoc routing protocol is a convention, or standard, or set of rules that controls how nodes decide which way to route packets between routing devices in a mobile ad hoc network. In the MANETs, all the nodes moves freely without knowing their networks topology and design, so they have to discover network topology on their own. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. Security has become a primary concern inorder to provide protected communicationbetween mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristicsof mobile ad hoc networks pose a numberof nontrivial challenges to security design,such as open peer-to-peer network architecture,shared wireless medium, stringent resource constraints,and highly dynamic network topology.These challenges clearly make a case for buildingmultifence security solutions that achieveboth broad protection and desirable networkperformance. In this article we focus on the fundamentalsecurity problem of protecting themultihop network connectivity between mobilenodes in a MANET. We identify the securityissues related to this problem, discuss the challengesto security design, and review the state-of-the-art security proposals that protect theMANET link- and all the layer operations ofdelivering data over the multihop wirelesschannel. The complete security solution shouldspan both layers, and encompass all three securitycomponents of prevention, detection, and reaction. Information is the heart of any business or industry. It provides sustenance toorganizational units: empowering and strengthening its users as groups andindividuals. It can be used for or against us, naturally concerning us with thesafety and integrity of our information. If the nature of our information is to bedistributed for accessibility then so must our efforts to secure it.Over the past two decades, the distributed computing industry has utilized theInternational Standards Organization's (ISO) Open System Interconnection (OSI)Model for better standardization of hardware and software components.Some layers have more impact than others when securing information.Networking is a prime concern for information security. The ubiquitous nature of network connectivity may let us access the world from our computer, but it also lets that same world gain access back to us in ways we may not desire.Today's network engineer has no choice but to be security-conscious, and the securityengineer has no choice but to understand the network he is tasked to secure. A great deal of formalized study has been devoted to the science and methodology of designing and maintaining networks. One formal system that network engineers discuss and apply frequently is the OSI Seven Layer Model for Networking, developed by the ISO (International Standards Organization) to define a standardized method for designing networks

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

and the functions that support them. This model describes seven layers of interaction for an information system communicating over a network, presenting a stack of layers representing major function areas that are generally required or useful for data communication between nodes in a distributed environment. Starting from a high-level application perspective, data is sent down the stack layer by layer, each layer adding information around the originally presented data until that original data plus its layers of added content are represented at the bottommost layer as a physical medium such as bursts of colored light or voltage across a wire in order for that data to physically travel from one point to the other in the real world. Together, they can be used to build a comprehensive solution. Utilizing the OSIModel's seven layers, this paper will demonstrate a logical, comprehensive andachievable approach tosecuring an organization's information resources. Actually in this paper first of all we tried to discuss the Security issues layer wise.Secondly layer wise problems and possible remedies in detail. Finally we have given the conclusion and future work.

II. SECURITY ISSUES LAYER WISE

A MANET provides network connectivity between mobile nodes over potentially multi hop wireless channels mainly through link-layer protocols that ensure one-hop connectivity, and network-layer protocols that extend the connectivity to multiple hops. These distributed protocols typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications. The main network-layer operations in MANETs are ad hoc routing and data packet forwarding, which interact with each other and fulfil the functionality of delivering packets from the source to the destination. The ad hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination. Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. While a comprehensive enumeration of the attacks is out of our scope, such network-layer vulnerabilities generally fall into one of two categories [11][12]:

Layer	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Presentation Layer	Cryptographic flaws may be exploited to circumvent privacy protections
Session Layer	Session identification may be subject to spoofing and hijack
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Data Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

Routing attacks and packet forwarding attacks, based on the target operation of the attacks.
The family of routing attacks refers to any action of advertising routing updates that does not follow the specifications of the routing protocol. The specific attack behaviours are related to the routing protocol used by the MANET. For example, in the context of DSR [2], the attacker may modify the source route listed in the REQ or RREP packets by deleting a node from the list, switching the order of nodes in the list, or appending a new node into the list [5]. When distance-vector routing protocols such as AODV [1] are used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from other nodes [6]. By attacking the routing protocols, the attackers can attract

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

traffic toward certain destinations in the nodes under their control, and cause the packets to be forwarded along a route that is not optimal or even non-existent. The attackers can create routing loops in the network, and introduce severe network congestion and channel contention in certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, and partition the network in the worst case. There are still active research efforts in identifying and defeating more sophisticated and subtle routing attacks. For example, the attacker may further subvert existing nodes in the network, or fabricate its identity and impersonate another legitimate node [7]. A pair of attacker nodes may create a wormhole [8] and shortcut the normal flows between each other. In the context of on-demand ad hoc routing protocols, the attackers may target the route maintenance process and advertise that an operational link is broken [5]. In addition to routing attacks, the adversary may launch attacks against packet forwarding operations as well. Such attacks do not disrupt the routing protocol and poison the routing states at each node. Instead, they cause the data packets to be delivered in a way that is intentionally inconsistent with the routing states. For example, the attacker along an established route may drop the packets, modify the content of the packets, or duplicate the packets it has already forwarded. Another type of packet forwarding attack is the denial-of-service (DoS) attack via network-layer packet blasting, in which the attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET. Recent research efforts have also identified the vulnerabilities of the link-layer protocols, especially the de facto standard IEEE 802.11 MAC protocol [3], for MANETs. It is well known that 802.11 WEP is vulnerable to several types of cryptography attacks due to the misuse of the cryptographic primitives [9]. The 802.11protocol is also vulnerable to DoS attacks targeting its channel contention and reservation schemes. The attacker may exploit its binary exponential back off scheme to deny access to the wireless channel from its local neighbours [10]. Because the last winner is always favoured among local contending nodes, a continuously transmitting node can always capture the channel and cause other nodes to back off endlessly. Moreover, back offs at the link layer can incur a chain reaction in upper layer protocols using back off schemes (e.g., TCP's window management). Another vulnerability of 802.11 comes from the NAV field carried in the request to send/clear to send (RTS/CTS) frames, which indicates the duration of channel reservation. An adversarial neighbour of either the sender or the receiver may overhear the NAV information and then intentionally introduce a 1-bit error into the victim's link-layer frame by wireless interference. The corrupted frame has to be discarded by the receiver after error detection. This effectively constitutes another type of DoS attack.

III. LAYER WISE PROBLEMS AND POSSIBLE REMEDIES

Physical Layer:
The physical layer is responsible for the physical communication between end stations. It is concerned with the actual encoding and transmission of data in electromechanical terms of voltage and wavelength [3, 4]. For purposes of information security we can widen this definition to apply to all physical world factors, such as physical media and input device access, power supply, and any other issue bounded by physical terms.

Physical Layer problems:
The problems or attacks faced by the physical layer are Loss of Power, Loss of Environmental Control, Physical Theft of Data and Hardware, Physical Damage or Destruction of Data and Hardware, Unauthorized changes to the functional environment (data connections, Removable media, adding/removing resources), Disconnection of Physical Data Links, Undetectable Interception of Data Keystroke & Other Input Logging.

Possible Remedies for Physical Layer:
We can have the control on physical layer by locking perimeters and enclosures, Electronic lock mechanisms for logging & detailed authorization, Video & Audio Surveillance, PIN & password secured locks, Biometric authentication systems, Data Storage Cryptography and Electromagnetic Shielding.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Data Link Layer:
The Data Link Layer is concerned with the logical elements of transmissions between two directly connected stations. It deals with issues of local topology where many stations may share a common local media. This is the layer where data packets are prepared for transmission by the physical layer. The data link layer is the realm of MAC addresses and VLANs as well as WAN protocols such as Frame Relay and ATM. Switch issues such as broadcast and collision domains are a layer two concern. It is also the realm of wireless protocols such as the various flavours of 802.11 wireless networking .For discussion purposes we will consider layer two to pertain to any direct data transmission issue, including modems, wireless and WAN circuits.

Data Link Layer problems:
The problems created by the attackers in the Data Link Layer are MAC Address Spoofing (station claims the identity of another), VLAN circumvention (station may force direct communication with other stations, bypassing logical controls such as subnets and firewalls.),
Spanning Tree errors may be accidentally or purposefully introduced, causing the layer two environments to transmit packets in infinite loops. In wireless media situations, layer two protocols may allow free connection to the network by unauthorized entities, or weak authentication and encryption may allow a false sense of security. Switches may be forced to flood traffic to all VLAN ports rather than selectively forwarding to the appropriate ports or allowing interception of data by any device connected to a VLAN.

Possible Remedies for Data Link Layer:
With the following precautionary measures we can have the control on Data Link Layer. MAC Address Filtering- Identifying stations by address and cross-referencing physical port or logical access. Do not use VLANs to enforce secure designs. Layers of trust should be physically isolated from one another, with policy engines such as firewalls between. Wireless applications must be carefully evaluated for unauthorized access exposure. Built-in encryption, authentication, and MAC filtering may be applied to secure networks.

Network Layer:
The Network layer is concerned with the global topology of the internet work - it is used to determine what path a packet would need to take to reach a final destination over multiple possible data links and paths over numerous intermediate hosts. This layer typically uses constructs such as IP addresses to identify nodes, and routing tables to identify overall paths through the network and the more immediate next-hop that a packet may be forwarded to. Protocols such as ARP facilitate that process, giving layer two mapping to layer three addresses, and telling layer three what link-layer path should be taken to follow its routing table's indication of the appropriate path. In the opposite direction, protocols such as IP will identify their higher-level layer four transmission protocol such as TCP or UDP in order to direct layer four as to how the incoming data should be handled.

Network Layer problems:
Network layer is the heart of the transmission layers when we talk about Routing. So it is very important to have more focus and research on how to protect this layer from the attackers. Here is the some information about the attacks like Route spoofing - propagation of false network topology, IP Address Spoofing- false source addressing on malicious packets, Identity & Resource ID Vulnerability - Reliance on addressing to identify resources and peers can be brittle and vulnerable.

Possible Remedies for Network Layer:
Here are the some ideas to have the control on Network layer. Route policy controls - Use strict anti-spoofing and route filters at network edges, Firewalls with strong filter & anti-spoof policyARP/Broadcast monitoring software, Implementations that minimize the ability to abuse protocol features such as broadcast etc.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Transport Layer:
The Transport Layer is concerned with the transmission of data streams into the concerned lower layers of the model, taking data streams from above and packaging them for transport, and with the reassembly and passing of incoming data packets back into a coherent stream for the upper layers of the model. Transport protocols may be designed for high reliability and use mechanisms to ensure data arrives complete at its destination, such as the TCP protocol, or protocols may choose to reduce overhead and simply depend upon the best efforts of the lower layers to deliver the data, and the protocols of the upper layers to ensure success to the levels they require, such as with the UDP protocol. Transport protocols may implement flow control, quality of service, and other data stream controls to meet their transmission needs.

Transport Layer problems:
The problems Related to the Transport layer are as follows:
Mishandling of undefined, poorly defined, or "illegal" conditions, Differences in transport protocol implementation allow "fingerprinting' and other enumeration of host information, Overloading of transport-layer mechanisms such as port numbers limit the ability, to effectively filter and qualify traffic. Transmission mechanisms can be subject to spoofing and attack based on crafted packets and the educated guessing of flow and transmission values, allowing the disruption or seizure of control of communications.

Possible Remedies for Transport Layer:
We can have the control on Transport layer with the given possible measures.
Strict firewall rules limiting access to specific transmission protocols and sub protocol information such as TCP/UDP port number or ICMP type, State full inspection at firewall layer, preventing out-of-state packets, "illegal" flags, and other phony packet profiles from entering the perimeter, stronger transmission and layer session identification mechanisms to prevent the attack and takeover of communications

Session Layer:
The Session Layer is concerned with the organization of data communications into logical flows. It takes the higher layer requests to send data and organizes the initiation and cessation of communication with the far end host. The session layer then presents its data flows to the transport layer below where actual transmission begins. Session protocols will often deal with issues of access and accessibility, allowing local applications to identify and connect to remote services, and advertising services to remote clients and dealing with subsequent requests to connect. The session layer also deals with higher-order flow control from an application perspective; just as the transport layer may control transmission from a network-oriented perspective and limit the flow to match the available network capacity, the session layer may control the flow up through to the application layer and limit the rate that data enters or leaves that realm based on arbitrary or dynamic limits.

Session Layer problems:
The problems faced at the Session layer are described here.
Weak or non-existent authentication mechanisms, passing of session credentials such as user ID and password in the clear, allowing intercept and unauthorized use, Session identification may be subject to spoofing and hijack, Leakage of information based on failed authentication attempts, unlimited failed sessions allow brute-force attacks on access credentials.

Possible Remedies for Session Layer:
We can overcome the problems present in the Session layer with Encrypted password exchange and storage, Accounts have specific expirations for credentials and authorization, Protect session identification information via random/cryptographic means, and Limit failed session attempts via timing mechanism, not lockout.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Presentation Layer:
The Presentation Layer deals with the organization of data passed from the application layer into the network. This layer allows for the standardization of data and the communication of data between dissimilar hosts, such as platforms with different binary number representation schemes or character sets (ASCII vs. UNICODE, for example.) Presentation Layer protocols typically rely upon a standardized data format for use on the network, and various conversion schemes to convert from the standardized format into and out of specific local formats. The Presentation Layer can also control network-layer enhancements such as compression or encryption.

Presentation Layer problems:
The Vulnerabilities present in the Presentation layer are Poor handling of unexpected input can lead to application crashes or surrender of control to execute arbitrary instructions. Unintentional or ill-advised use of externally supplied input in control contexts may allow remote manipulation or information leakage. Cryptographic flaws may be exploited to circumvent privacy protections.

Possible Remedies for Presentation Layer:
To have the control on Presentation layer and to save from the attacks we can take the following precautionary measures. Careful specification and checking of received input incoming into applications or library functions, Separation of user input and program control functions- input should be sanitized and sanity checked before being passed into functions that use the input tocontrol operation, Careful and continuous review of cryptography solutions to ensure currentsecurity versus know and emerging threats.

Application Layer:
The Application Layer deals with the high-level functions of programs that mayutilize the network. User interface and primary function live at this layer. All functionsnot pertaining directly to network operation occur at this layer.

Application Layer problems:
Application layer have some loopholes which can leads towards attacks. Those loopholes are open design issues allow free use of application resources by unintended parties, Backdoors and application design flaws bypass standard security controls, inadequate security controls force “all-or-nothing” approach, resulting in either excessive or insufficient access. Overly complex application security controls tend to be bypassed or poorly understood and implemented. Program logic flaws may be accidentally or purposely used to crash programs or cause undesired behaviour.

Possible Remedies for Application Layer:
Application level access controls to define and enforce access to application resources. Controls must be detailed and flexible, but also straightforward to prevent complexity issues from masking policy and implementation weakness, Standards, testing, and review of application code and functionality-A baseline is used to measure application implementation and recommend improvements, IDS systems to monitor application inquiries and activity Some host-based firewall systems can regulate traffic by application, preventing unauthorized or covert use of the network.

IV. CONCLUSION AND FUTURE WORK

In this article we focus on the fundamental security problem of protecting the multihop network connectivity between mobile nodes in a MANET. We identify the security issues related to this problem, discuss the challenges to security design, and review the state-of-the-art security proposals that protect the MANET link- and all the layer operations of delivering data over the multihop wireless channel.Moreover In this paper we have given the complete overview on the problems and possible remedies for each layer which will help to improve the security in each layer. In future we will work separately on Security issues layer wise.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

REFERENCES

[1] C. Perkins and E Royer, "Ad Hoc On-Demand Distance Vector Routing", 2nd IEEE Work shop on Mobile Comp. Sys.AndApps, Version.2, pp. 90-100, 1999.
[2] D. Johnson and D. Maltz"Dynamic Source Routing in Ad Hoc Wireless Networks", MobileComputing, The Kluwer international series in Engineering, Volume 353, pp.153-181, 1996.
[3] S Northcutt, L Zeltzer, S Winters, KK Fredrick, and RW Ritchey, "Inside Network Perimeter Security", New Riders, p 4, 2003.
[4] E Cole, J Fossen, S Northcutt, and H Pomeranz, "SANS Security Essentials with CISSP CBK", SANS Press, pp.257-258, 2003.
[5] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks", Springer Science, Wireless Networks, Volume 11,pp.21-38, 2005.
[6] M. Zapata, and N. Asokan, "Securing Ad Hoc Routing Protocols,",WiSE '02 Proceedings of the 1st ACM workshop on Wireless security,pp.1-10,2002.
[7] K.Sanzgiri,, B.Dahilly, B. Neil Leviney, C.Shieldsz, E.M. Belding-Royer"A Secure Protocol for Ad Hoc Networks,",Proceedings of the 10 th IEEE International Conference on Network Protocols (ICNP'02), 2002.
[8] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," IEEE INFOCOM, 2003.
[9] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," ACM MOBICOM, 2001.
[10] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," IEEE MILCOM, volume 2, pp.1118-1123,2002.
[11] Hao Yang, HaiyunLuo, Fan Ye, Songwu Lu, And Lixia Zhang," Security In Mobile Ad Hoc Networks: Challenges And Solutions" IEEE Wireless Communications •, Volume 11, pp.38-47, 2004.
[12] AsifShabbir, Fayyaz Khalid, Syed MuqsitShaheed, Jalil Abbas, M. Zia-Ul-Haq," Security: A Core Issue in MobileAd hoc Networks" Journal of Computer and Communications,volume 3,pp.41-66,2015