© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

Review On Securing Of Wireless Mesh Network From Denial Of Services

[1]Mukesh Kumar, Research Scholar, Department of CSE, CBS group of Institutions Jhajhar
[2]Pooja Dhankhar , assistant professor, Department of CSE, CBS group of institutions jhajhar

ABSTRACT: A wireless mesh network is a communications network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. In our research we have discussed security issues related to Wireless Network. The distributed network computing model allows all network computer system systems to take part within processing but at their respective ends, separately. This model allows sharing data & services but does not help other network computer system systems within processing. The objectives of research are to establishment of Distributed Network Environment & creation of Wireless mesh within this Distributed Environment. After that we will study of Existing Security loop holes within wireless mesh based distributed network environment. Then we will create a new security mechanism to enhance security of data on wireless mesh network by customizing existing Encryption & Decryption Mechanisms. The main objective is to boost outer layer security by enhancing packet filter mechanism.

[1] INTRODUCTION

Wireless Mesh Network

The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may, but need not, be connected to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh networks can self form and self heal. Wireless mesh networks can be implemented with various wireless technologies including 802.11, 802.15, 802.16, cellular technologies and need not be restricted to any one technology or protocol.

Architecture

Wireless mesh architecture is a first step towards providing cost effective and dynamic high-bandwidth networks over a specific coverage area. Wireless mesh infrastructure is, in effect, a network of routers minus the cabling between nodes. It's built of peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points (AP) do. Mesh infrastructure carries data over large distances by splitting the distance into a series of short hops. Intermediate nodes not only boost the signal, but cooperatively pass data from point A to point B by making forwarding decisions based on their knowledge of the network, i.e. perform routing. Such architecture may, with careful design, provide high bandwidth, spectral efficiency, and economic advantage over the coverage area. Wireless mesh networks have a relatively stable topology except for

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

the occasional failure of nodes or addition of new nodes. The path of traffic, being aggregated from a large number of end users, changes infrequently. Practically all the traffic in an infrastructure mesh network is either forwarded to or from a gateway, while in ad hoc networks or client mesh networks the traffic flows between arbitrary pairs of nodes.

Applications

Mesh networks may involve either fixed or mobile devices. The solutions are as diverse as communication needs, for example in difficult environments such as emergency situations, tunnels, oil rigs, battlefield surveillance, high-speed mobile-video applications on board public transport or real-time racing-car telemetry. An important possible application for wireless mesh networks is VoIP. By using a Quality of Service scheme, the wireless mesh may support local telephone calls to be routed through the mesh.

[2] LITERATURE REVIEW

Between 1991 & 1994, simplicity & effectiveness of early technologies used to surf & exchange data through World Wide Web helped to port them to many different operating systems & spread their use among scientific organizations & universities, & then to industry. In 1994 Tim Berners-Lee decided to constitute World Wide Web Consortium (W3C) to regulate further development of many technologies involved (HTTP, HTML, etc.) through a standardization process.

In 2006 Wormhole Attacks within Wireless Networks Yih-Chun Hu, *Member, IEEE,* Adrian Perrig, *Member, IEEE,* & David B. Johnson, *Member, IEEE*[4]

As mobile ad hoc network applications are deployed, security emerges as a central requirement. In this paper, we introduce *wormhole attack*, a severe attack within ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if attacker has not compromised any hosts, & even if all communication provides authenticity & confidentiality. In thewormhole attack, an attacker records packets (or bits) at one location within network, tunnels them (possibly selectively) to another location, & retransmits them there into network.

The wormhole attack could form a serious threat within wireless networks, especially against many ad hoc network routing protocols & location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. We present a general mechanism, called *packet leashes*, for detecting and, thus defending against wormhole attacks, & we present a specific protocol, called TIK, that implements leashes.We also discuss topology-based wormhole detection, & show that it is impossible for these approaches to detect some wormhole topologies.

In 2006 IEEE 802.11 Wireless LAN Security Overview was introduced by *Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen*[1]

Wireless Local Area Networks (WLANs) are cost effective & desirable gateways to mobile computing. They allow computers to be mobile, cable less & communicate with speeds close to speeds of wired LANs. These features came with expensive price to pay within areas of security of network. This paper

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

identifies & summarizes these security concerns & their solutions. Broadly, security concerns within WLAN world are classified into physical & logical. The paper overviews both physical & logical WLANs security problems followed by a review of main technologies used to overcome them. It addresses logical security attacks like maninthe-middle attack & Denial of Service attacks as well as physical security attacks like rouge APs. Wired Equivalent Privacy (WEP) was first logical solution to secure WLANs. However, WEP suffered many problems which were partially solved by IEEE802.1x protocol. Towards perfection within securing WLANs, IEEE802.11i emerged as a new MAC layer standard which permanently fixes most of security problems found within WEP & other temporary WLANs security solutions. This paper reviews all security solutions starting from WEP to IEEE802.11i & discusses strength & weakness of these solutions.

IN 2010 SECURITY AND PRIVACY IN EMERGING WIRELESS NETWORKS ARTICLE WAS WRITTEN BY DI MA UNIVERSITY OF MICHIGAN-DEARBORN[2]

Wireless communication is continuing to make inroads into many facets of society & is gradually becoming more & more ubiquitous. While within past wireless communication (as well as mobility) was largely limited to first & last transmission hops, today's wireless networks are starting to offer purely wireless, often mobile, & even opportunistically connected operation. The purpose of this article was to examine security & privacy issues within some new & emerging types of wireless networks, & attempt to identify directions for future research.

[3] OBJECTIVE OF RESEARCH

The objectives of research are as follow:

1. Establishment of Wireless Network Environment
2. Creation of distributed network within this Wireless Environment
3. Study of Existing Security loop holes within Wireless network.
4. Enhancing security by customizing existing Encryption & Decryption Mechanisms.
5. Enhancing outer layer security by enhancing packet filter mechanism.

[4] TOOLS AND TECHNOLOGY

Packet Filters

Packet filters may be set up on routers, firewalls, & servers to accept or deny packets from services & specific addresses. And packet filters augment authentication & authorization mechanisms. They help shield network resources from theft, unauthorized use, DoS attacks & destruction.

The first policy requires a thorough understanding of specific security attacks & may be hard to implement. The second policy is easier to implement & more secure since security proprietor does not have to guess future attacks for which packets should be denied. second policy is also easier to test since there is a finite set of accepted uses of network. To do a decent job implementing second policy requires a decent understanding of network requirements. network designer should work with security administrator to determine what types of packets should be accepted.

Cisco implements second policy within its packet filters, which Cisco calls ACL (access control lists). ACL on a switch or router running Cisco IOS Software always has an implicit deny-all statement at

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

end. Specific accept statements are processed before implicit deny-all statement. (The statement is implicit since administrator does not have to actually enter it, although it is a decent idea to enter it to make behavior of list more obvious.)

ACLs let you control whether network traffic is forwarded or blocked at interfaces on a router or switch. ACL definitions provide criteria which are applied to packets which enter or exit an interface. Typical criteria are packet source address, packet destination address, or upper-layer protocol within packet.

Because Cisco IOS Software tests a packet against each criteria statement within list until a match is found, ACLs should be designed with care to provide decent performance. By studying traffic flow, you may design list so which most packets match earliest conditions. Less conditions to checked per packet means improved throughput. Decent advice for designing ACLs is to order list with most general statements at top & most specific statements at bottom, with last statement being general, implicit deny-all statement.

[5] PROBLEM STATEMENT

The major problem is network security against attackers & hackers. Network Security includes two basic securities.

- The first is security of data info i.e. to protect data info from unauthorized access & loss.
- And second is computer system security i.e. to protect data & to thwart hackers.

Here network security not only means security within a single network rather within any network or network of networks. Now our requirement of network security has broken into two needs. One is requirement of data info safety & other is requirement of computer system security. On internet or any network of an organization, thousands of important data info is exchanged daily. This data info may be misused by attackers.

Data info security is needed for following given reasons:

- To protect secret data info users on net only. No other person should watcher access it.
- To protect data info from unwanted editing, accidently or intentionally by unauthorized users.
- To protect data info from loss & make it to be delivered to its destination properly.
- To manage for acknowledgement of message received by any node within order to protect from denial by despatcher within specific situations. e.g. let a customer orders to obtaining a few shares XYZ to broader & denies for order after two days as rates go down.
- To restrict a user to deliver many message to another user with name of a third one. e.g. a user X for his own notice makes a message containing many favorable instructions & sends it to user Y within these a manner which Y accepts message as coming from Z, manager of association.
- To protect message from undesirable delay within transmission lines/route within order to deliver it to required destination within time, within case of urgency.
- To protect data from wandering data packets or data info packets within network for infinitely long time & thus increasing

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

congestion within line within case destination machine fails to capture it since of many internal faults.

Types of Network Security Attacks

We may group network attacks by skills possessed by attacker. Based on these criteria we may divide attacks within following categories:

- Unstructured – attacks made by unskilled hackers. Singles behind these attacks use hacking tools accessible on Internet & are usually not aware of environment they are attacking. These attacks should not be neglected since they may expose precious data info to malicious users.
- Structured – Massive attacks made by singles who possess advanced computing skills. these hackers are experts within exploiting system vulnerabilities. By gaining enough data info about a company's network, these singles may create custom hacking tools to break network security. Maximum structured attacks are done by singles with decent programming skills & a decent understanding of system's operating systems, networking & so on.
- Social engineering – One another type of network attack. Malicious users take advantage of human's sincerity & usually gain significant data info directly from their victims. They usually call or deliver falsified emails to their sufferers pretending to be many other people totally.
- Phishing is a method which is pretty cool to implement by hackers. This paragraph describes phishing attacks: "Phishing is act of attempting to acquire data info these as usernames, passwords, & credit card details (and sometimes indirectly, money) by masquerading as a trustworthy entity within an electronic communication". Entire sites are known to be duplicated by hackers within an attempt to steal precious data info from users.

In today's data networks there are many different types of attacks & each one requires special skills which hackers must poses within order to successfully crack into somebody's privacy:

- Eavesdropping – It is one of most common types of attacks. A malicious user may gain critical data info from "listening" to network traffic. since most data transmit ion are sent unencrypted, there are many cases within which traffic is susceptible to interception. traffic may be analyzed using sniffing tools (also known as snooping) to read data info as it is sent into network. Wireless networks are more susceptible to interception than wired ones. Eavesdropping may be prevented by using encryption algorithms.
- Dos & DDoS attacks (Denial of Service & Distributed Denial of Service attacks) – In these type of attacks take advantage of network traffic to create abnormal behavior to network services or applications. Servers are usually targeted & flooded with data until they become unreachable. Core network equipment may be blocked & thus preventing normal traffic from flowing into network. Distributed denial of service attacks are more dangerous since attacks are made from multiple sources.

[6] PROPOSED WORK

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

(A) Distributed Network Environment Establishment:

- **Topology:** Star Network
- **Media of transmission :** Wifi
- **Number of Systems:** 4
- **Operating system :** Windows

(B) Establishment of server:

- Webhost for PHP(Apache web server)
- Webhost of ASP.NET (IIS server)
- Database server (Sql server/My Sql)

(C) Study of Existing Security loop holes within server

- Denial of Service & Distributed Denial of Service attacks
- Brute Force attack
- Threat from Cryptanalyst
- Threat from Hacker

(D) Enhancing security by customizing existing Encryption & Decryption Mechanisms

- Development of Basic Encryption & decryption code within Java Socket programming.
- Enhancing security of cryptography by making key stronger for authentic encryption decryption.

(E) Enhancing outer layer security by enhancing packet filter mechanism

Packet Filter Mechanism would also be enhanced by introducing user defined algorithm to ignore packets from black listed Internet

[7] FUTURE SCOPE

As security mechanism is user defines so further security layer could be added within future. Such security mechanism may be applicable of other server like FTP Server, telnet, SMTP Server.

[8] CONCLUSION

Hackers use viruses, Trojans & worms to infect devices & gain important data info. Our security mechanism will first prevent hacker to access data within unauthenticated way & restrict them to understand data.

REFERENCES

[1]IEEE 802.11 Wireless LAN Security Overview by Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen, Department of Electrical & Computer Engineering – Sultan Qaboos University, Oman. IJCSNS International Journal of Computer Science & Network Security, VOL.6 No.5B, May 2006

[2] SECURITY AND PRIVACY IN EMERGING WIRELESS NETWORKS BY DI MA UNIVERSITY OF MICHIGAN-DEARBORN, IEEE Wireless Communications October 2011

[3] Efficient Gossip Protocols for Verifying Consistency of Certificate Logs by Laurent Chuat ETH Zurich, Pawel Szalachowski ETH Zurich

[4] Attacks within Wireless Networks Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, & David B. Johnson, Member, IEEE, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[5] Lightweight Hidden Services by Andriy Panchenko, Otto Spanioly, Andre Egnersy, & Thomas Engel Computer Science department, RWTH Aachen University, Germany within June 2011

[6] In 2011 PFS: Probabilistic Filter Scheduling Against Distributed Denial-of-Service Attacks

36th Annual IEEE Conference on Local Computer Networks, 978-1-61284-927-0/10/$26.00 ©2011 IEEE

[7] D. K. Y. Yau, J. C. S. Lui, F. Liang, & Y. Yam, "Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles," IEEE/ACM Trans. Netw., vol. 13, no. 1, pp. 29–42, 2005.

[8] X. Yang, D. Wetherall, & T. E. Anderson, "TVA: a DoS-limiting network architecture," IEEE/ACM Trans. Netw., vol. 16, no. 6, pp. 1267–1280, 2008.

[9] M. Sung & J. Xu, "IP traceback-based intelligent packet filtering: A novel technique for defending against internet DDoS attacks," IEEE Trans. Parallel Distrib. Syst., vol. 14, no. 9, pp. 861–872, 2003.

[10] S. Savage, D. Wetherall, A. Karlin, & T. Anderson, "Practical Network Support for IP Traceback," within Proc. of ACM SIGCOMM, Aug. 2000, pp.295–396.