ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

Security Issues and Attacks in Wireless Ad Hoc Networks

K.Murugan, Dr.P.Suresh (Supervisor)

Research Scholar, Bharathiar University & Assistant Professor in Computer Science, Govt. College for Women, Kolar, Karnataka, India,

HOD, Department of Computer Science, Salem Sowdeswari College, Salem, Tamil Nadu, India,

ABSTRACT: Wireless networking technologies range from global voice and data networks, which allow users to establish wireless connections across long distances, to infrared light and radio frequency technologies that are optimized for short-range wireless connections. Devices commonly used for wireless networking include portable computers, desktop computers, hand-held computers, personal digital assistants (PDAs), cellular phones, pen based computers, and pagers. Wireless technologies serve many practical purposes. For example, mobile users can use their cellular phone to access e-mail. Travelers with portable computers can connect to the Internet through base stations installed in airports, railway stations, and other public locations. At home, users can connect devices on their desktop to synchronize data and transfer files.

To lower costs, ensure interoperability, and promote the widespread adoption of wireless technologies, organizations such as the Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), Wireless Ethernet Compatibility Alliance (WECA), and the International Telecommunication Union (ITU) are participating in several major standardization efforts. For example, IEEE working groups are defining how information is transferred from one device to another (whether radio waves or infrared light is used) and how and when a transmission medium should be used for communications. In developing wireless networking standards, organizations such as the IEEE address power management, bandwidth, security, and issues that are unique to wireless networking.

KEYWORDS*:* Wireless, Security, Threats, Attacks, Authentication

I. SECURITY ISSUES

1.1 IEEE 802 Security

Wireless devices seem to be everywhere these days, and wireless "hotspots" are popping up worldwide. 802.11 is a group of specifications developed by the Institute of Electrical and Electronics Engineers(IEEE) for wireless local area networks (WLANs). When talking about security there is no such thing as having a completely secure system. Everything is insecure to some degree or other. The degree of security we require is dictated by the sensitivity of the information we possess.

If we require very high levels of security then we cannot rely on the built-in security measures of a Wi-Fi network alone. On the other hand, most small to medium sized companies do not require very high levels of security, in which case we may use the standard Wi-Fi security measures. If we already have a wireless network we may be concerned about whether it is secure. Securing information from unauthorized access is a major problem for any network. Broadly security can be classified as:

- Network security
- System security
- Information security
- Physical security

Security is made up of a suite of multiple technologies that solve numerous authentication, information integrity, and identification problems. It includes the following technologies: firewalls, authentication servers, biometrics, cryptography, intrusion detection, virus protection, and Virtual Private Networks.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

1.2 Security Threats

Easy Access: 802.11 require that networks periodically announce their existence to the world with special frames called Beacons. However, the information needed to join a network is also the information needed to launch an attack on a network. Beacon frames are not processed by any privacy function, which means that our 802.11 network and its parameters are available for anybody with an 802.11 card. "War drivers" have used high-gain antennas and software to log the appearance of Beacon frames and associate them with a geographic location using Global Positioning System. Short of moving into heavily shielded office space that does not allow RF signals to escape, there is no solution for this problem. The best we can do is to mitigate the risk by using strong access control and encryption solutions to prevent a wireless network from being used as an easy entry point into the network. We should deploy access points outside firewalls, and protect sensitive traffic with Virtual Private Networks.

Rogue Access Points:"Rogue" access points deployed by end users pose great security risks. Most existing small deployments mapped by war drivers do not enable the security features on products, and many access points have had only minimal changes made to the default settings. It is hard to believe that end users within a large corporation will do much better. Tools like Net Stumbler allow network administrators to wander their building looking for unauthorized access points, but it is expensive to devote time to wandering the building looking for new access points. Monitoring tools will also pick up other access points in the area, which may be a concern if we are sharing a building or a floor with another organization. Their access points may cover part of our floor space, but their access points do not directly compromise our network and are not cause for alarm. The periodic "walk-through" of the campus is the only way to address the threat of unauthorized deployment.

Unauthorized Use of Service: A clear majority of access points are put in service with only minimal modifications to their default configuration. Nearly all of the access points running with default configurations have not activated WEP (Wired Equivalent Privacy) or have a default key used by all the vendor's products. Two problems can result from such open access. In addition to bandwidth charges for unauthorized use, legal problems may result. Unauthorized users may not necessarily obey our service provider's terms of service, and it may take only one spammer to cause our ISP to revoke our connectivity.

Service and Performance Constraints: Wireless LANs have limited transmission capacity. Networks based on 802.11b have a bit rate of 11 Mbps, and networks based on the newer 802.11a technology have bit rates up to 54 Mbps. This capacity is shared between all the users associated with an access point. Due to MAC-layer overhead, the actual effective throughput tops out at roughly half of the nominal bit rate. It is not hard to imagine how local area applications might overwhelm such limited capacity, or how an attacker might launch a denial of service attack on the limited resources. Radio capacity can be overwhelmed in several ways. It can be swamped by traffic coming in from the wired network at a rate greater than the radio channel can handle. If an attacker were to launch a ping flood from a Fast Ethernet segment, it could easily overwhelm the capacity of an access point. Depending on the deployment scenario, it might even be possible to overwhelm several access points by using a broadcast address as the destination of the ping flood.

MAC Spoofing and Session Hijacking: Every frame has a source address, but there is no guarantee that the station sending the frame actually put the frame "in the air." There is no protection against forgery of frame source addresses. Attackers can use spoofed frames to redirect traffic and corrupt ARP tables. At a much simpler level, attackers can observe the MAC addresses of stations in use on the network and adopt those addresses for malicious transmissions. To prevent this class of attacks, user authentication mechanisms are being developed for 802.11 networks. By requiring authentication by potential users, unauthorized users can be kept from accessing the network. (Denial of service attacks will still be possible, though, because nothing can keep attackers from having access to the radio layer.)

Traffic Analysis and Eavesdropping:802.11 standards provide no protection against attacks that passively observe traffic. The main risk is that 802.11 do not provide a way to secure data in transit against eavesdropping. Frame headers are always "in the clear" and are visible to anybody with a wireless network analyzer. Security against eavesdropping was supposed to be provided by the much-maligned Wired Equivalent Privacy specification. WEP protects only the initial association with the network and user data frames. Management and control frames are not encrypted or authenticated by WEP, leaving attacker wide latitude to disrupt transmissions with spoofed frames. If our wireless LAN is being used for sensitive data, WEP may very well be insufficient for our needs. Strong cryptographic solutions like SSH, SSL, and IPSec were designed to transmit data securely over public channels and have proven resistant to attack over many years, and will almost certainly provide a higher level of security.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

Higher Level Attacks: Once an attacker gains access to a wireless network, it can serve as a launch point for attacks on other systems. Many networks have a hard outer shell composed of perimeter security devices that are carefully configured and meticulously monitored. Inside the shell, though, is a soft, vulnerable center. Wireless LANs can be deployed quickly if they are directly connected to the vulnerable backbone, but that exposes the network to attack. Depending on the perimeter security in place, it may also expose other networks to attack. The solution would be to treat the wireless network as something outside the security perimeter, but with special access to the inside of the network. Although wireless LAN security can seem challenging, most of the challenges can be addressed by reasonable security precautions. Network designs will, of course, continue to be affected by the development of new technologies and user demands.

1.3 Attacks

We can classify attacks as passive or active.

Passive attacks: In a passive attack an unauthorized node monitors and aims to find out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

Active Attacks: These attacks cause unauthorized state changes in the network such as denial of service, modification of packets, and the like. These attacks are generally launched by users or nodes with authorization to operate within the network. We classify active attacks into four groups: dropping, modification, fabrication, and timing attacks. It should be noted that an attack can be classified into more than one group.

II. SECURITY REQUIREMENTS

The three basic security services defined by IEEE for the WLAN environment are:

- Authentication
- Confidentiality (Privacy)
- Integrity

Authentication: A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This provides access control to the network by denying access to client stations that cannot authenticate properly. The IEEE 802.11 specification defines two means to "validate" wireless users attempting to gain access to a wired network – open-system authentication and shared-key authentication.
Confidentiality (Privacy): Confidentiality or privacy was a second goal of WEP. It was developed to provide "privacy achieved by a wired network". The intent was to prevent information compromise from casual eavesdropping (passive attack). The 802.11 standard supports privacy (confidentiality) through the use of cryptographic techniques for the wireless interface. The WEP cryptographic technique for confidentiality also uses the RC4 symmetric key, stream cipher algorithm to generate a pseudo-random data sequence. This "key stream" is simply added modulo 2 (exclusive-OR-ed) to the data to be transmitted. Through the WEP technique, data can be protected from disclosure during transmission over the wireless link. WEP is applied to all data above the 802.11 WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hyper Text Transfer Protocol (HTTP). As defined in the 802.11 standard, WEP supports only a 40-bit cryptographic key size for the shared key. However, numerous vendors offer nonstandard extensions of WEP that support key lengths from 40 bits to 104 bits. At least one vendor supports a key size of 128 bits. The 104-bit WEP key, for instance, with a 24-bit Initialization Vector (IV) becomes a 128-bit RC4 key.
Integrity: Another goal of WEP was a security service developed to ensure that messages are not modified in transit between the wireless clients and the access point in an active attack. The IEEE 802.11 specification also outlines a means to provide data integrity for messages transmitted between wireless clients and access points. This security service was designed to reject any messages that had been changed by an active adversary "in the middle." This technique uses a simple encrypted Cyclic Redundancy Check (CRC) approach. As depicted in the diagram above, a CRC-32, or frame check sequence, is computed on each payload prior to transmission. The integrity-sealed packet is

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

then encrypted using the RC4 key stream to provide the cipher-text message. On the receiving end, decryption is performed and the CRC is recomputed on the message that is received. The CRC computed at the receiving end is compared with the one computed with the original message. If the CRCs do not equal, that is, "received in error," this would indicate an integrity violation (an active message spoofer), and the packet would be discarded. As with the privacy service, unfortunately, 802.11 integrity is vulnerable to certain attacks regardless of key size. In summary, the fundamental flaw in the WEP integrity scheme is that the simple CRC is not a cryptographically secure mechanism such as a hash or message authentication code. The IEEE 802.11 specification does not, unfortunately, identify any means for key management (life cycle handling of cryptographic keys and related material). Therefore, generating, distributing, storing, loading, archiving, auditing, and destroying the material is left to those deploying WLANs.

III. SECURE ROUTING

It is critical to form and organize the topology and determine the connectivity of the network. There are a few types attacks mounted on the routing protocols.

Routing table overflow: The adversary node advertises routes to non-existent nodes, to the authorized nodes present in the network. The objective is to cause an overflow of the routing table and prevent the creation of entries to authorized nodes.

Routing table poisoning: The compromised nodes send fictitious updates or modify genuine route update packets to other nodes. It may result in congestion or even inaccessible of the network.

Packet replication: The malicious node replicates stale packets to consume resources, e.g. bandwidth and battery power (sleep deprivation attack) of other nodes.

Route cache poisoning: Similar to routing table poisoning, an adversary can also poison the route cache to achieve objectives. It happens to on-demand routing protocol.

Rushing attack: An adversary floods the received Route Request packet to the network, in order to take position in other nodes' routing table. It can take the man-in-the-middle attacks later on.

IV. CONCLUSION

Wireless Network is a kind of Ad hoc network with mobile wireless nodes. Due to its special characteristics like open network boundary, dynamic topology and hop-by-hop communications wireless network faced with a variety of challenges. Since all nodes participate in communications and nodes are free to join and leave the network, security became the most important challenge in wireless network. In this paper, we have analyzed the security threats an ad hoc network faces and presented the security objectives that need to be achieved. On one hand, the security-sensitive applications of ad hoc networks require high degree of security; on the other hand, ad hoc networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad hoc networks. Based on the classification and description of attacks, defense and countermeasure are presented to handle the problems.

This paper represents to analyze the security threats, to understand the security requirements for ad hoc networks, and to identify existing techniques, as well as to propose new mechanisms to secure ad hoc networks. More work needs to be done to deploy these security mechanisms in an ad hoc network and to investigate the impact of these security mechanisms on the network performance.

REFERENCES

[1]. G.Singla and P. Kaliyar, "A Secure Routing Protocol for MANETs Against Byzantine Attacks, "Computer Networks & Communications (NetCom), Lecture Notes in Electrical Engineering, vol. 131,pp. 571-578, 2013.International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015

[2]. X.Lv and H. Li, "Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks," Information Security, IET, vol. 7, 2013.

[3]. S.a.A.k.G, H.o.d.R.m, and S. sharma, "A Comprehensive Review of Security Issues in Manets ,"International Journal of Computer Applications vol. 69 2013.

[4] F.R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks," EURASIP Journal on Wireless Communications and Networking - Special issue on wireless network security, 2013.

[5]. A.MISHRA, R. Jaiswal, and S. Sharma, " A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network," presented at the 3rd International Conference on Advance Computing Conference (IACC), 2013.

[6]. P.T. Tharani, K. Muthupriya, and C. Timotta, "Secured consistent network for coping up with gabrication attack in MANET," international journal of Emerging Technology and Advanced Engineering, vol. 3, 2013.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

[7] A.El-Sayed, "Clustering Based Group Key Management for MANET," Advances in Security of Information and Communication, Networks Communications in Computer and Information Science, vol. 381, pp. 11-26, 2013.
[8]. R.H.Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS Attacks in Mobile Ad Hoc Networks: A Survey," presented at the Second International Conference on Advanced Computing & Communication Technologies (ACCT), 2012
[9]. H.Nishiyama, T. Ngo, N. Ansari, and N. Kato, "On Minimizing the Impact of Mobility on Topology Control in Mobile Ad Hoc Networks," Wireless Communications, IEEE Transactions, 2012.
[10]. M.Salmanian and M. Li, "Enabling secure and reliable policy-based routing in MANETs," presented at the military communications conference, MILCOM, 2012.
[11]. M.Suguna and P. Subathra, " Establishment of stable certificate chains for authentication in mobile adhoc networks," presented at the International Conference on Recent Trends in Information Technology (ICRTIT), 2011.
[12]. S.Rana and A. Kapil, "Security-Aware Efficient Route Discovery for DSR in MANET," Information and Communication Technologies, Communications in Computer and Information Science, vol. 101, pp. 186-194, 2010.
[13]. IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010 ISSN: 1793-8236 "Performance analysis of AODV, DSR & TORA Routing Protocols" Anuj K. Gupta, Member, IACSIT, Dr. Harsh Sadawarti, Dr. Anil K. Verma
[14]. D.Sharma, P. G. Shah, and X. Huang, "Protecting from Attacking the Man-in-Middle in WirelessSensor Networks with Elliptic Curve Cryptography Key Exchange," presented at the NSS '10Proceedings of the Fourth International Conference on Network and System Security, 2010.
[15]. K.Vishnu, "A new kind of transport layer attack in wireless Ad Hoc Networks," presented at theInternational Conference on Wireless Communications, Networking and Information Security(WCNIS), 2010.

BIOGRAPHY

Mr. K. Murugan is an Assistant Professor and Head of the Department of Computer Science at Government College for Women, Kolar. His current area of research interest is Computer Networks and its applications. He has successfully guided 15 candidates for M.Phil. He has been teaching computer Science for the past 17 Years. He completed his Master Degree in Computer Science at Bharathidasan University, Master of Philosophy in Computer Science at Manonmaniam Sundaranar University, Master of Engineering in Computer Science and Engineering at Anna University.

Dr. P. Suresh is a Head, Department of Computer Science, Salem Sowdeswari College [Govt. Aided], Salem. He received the M.Sc., Degree from Bharathidasan University in 1995, M.Phil Degree from Manonmaniam Sundaranar University in 2003, M.S (By Research) Degree from Anna University, Chennai in 2008, PGDHE Diploma in Higher Education and Ph.D., Degree from Vinayaka Missions University in 2010 and 2011 respectively in Computer Science. He is an Editorial Advisory Board Member of Elixir Journal. His research interest includes Data Mining and Natural Language Processing. He is a member of Computer Science Teachers Association, New York.