INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN MANAGEMENT AND COMPUTER APPLICATIONS
VOL. 2, ISSUE 3, MARCH-2013 ISSN NO: 2319-7471

Attacks and Challenges in Wireless Networks A Literature survey

Amit Khajuria[1], Roshan Srivastava[2]
[1]M. Tech Scholar, Computer Science Engineering, Lovely Professional University, Punjab, India
[2]Asst Prof, Computer Science Engineering, Lovely Professional University, Punjab, India
[1]amitkhajuria8@gmail.com, [2]roshan.1686@lpu.co.in

Abstract: Wireless networks provide numerous benefits in real world. This can help businesses to increase their productivity, lower cost and effectiveness, increase scalability and improve relationship with business partners and attract customers. Communication in wireless network is critical and challenging issue. There are many different ways to overcome to imperfections native to wireless networks. This paper is designed to help you to understand and to assist to make wireless network secure and beneficial asset. It presents recent advance in attack and the challenges. Indeed, there are different reasons to deploy technology, but like most, it is not without risks and downfall.

Keywords: WSN, Infrastructure, AD-Hoc, Spoofing.

I. Introduction

Wireless networks have become an integral part of the digital society of this world due to the easiness of implementation and the lower cost in comparison to the wired networks. The features in wireless networks are largely due to proliferation of wireless networking and sensor hardware. Technologies allow wireless devices to make networking a viable option for personal, commercial industrial and military use. However, with these rapid advances in wireless networking and hardware technologies come with inherent vulnerabilities, creating potential for a wide variety of attacks on network services. Wireless networks continue to grow due to the fact that they are potentially low cost and effective (providing solutions to a number of real world challenges), the need for effective security mechanisms also grow. As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. It is more difficult to come up with security measures of protecting data that flows through the air. However, the security measures cannot be ignored just because of the difficulty. Therefore, security vulnerabilities in wirelessNetworks should be identified and protected. There are, in general, three types of wireless networks that are most common:

- Sensor
- Ad-hoc
- Infrastructure.

II. Types of Attacks

1. Attacks in WSN

1.1 Man in the Middle Attack

The MITM attack is a form of active eavesdropping in which the attackers makes independent connections with the victims and relay messages between them, making them believe that they are directly exchanging data to each other over a private connection. The attacker will be able to intercept all message exchanging.

1.2 Jamming

This is one of the Denials of service Attacks in which the third party attempts to disrupt the operation of the network by broadcasting a high-energy signal. Jamming attacks in wireless sensor networks, classifying them as constant (corrupts

packets as they transfer), deceptive (sends a constant stream of bytes into network to make it look like legitimate traffic), random (randomly alternates between sleep and jamming to save energy), and reactive (transmits a jam signal when it senses traffic).

1.3 Clone Attack

In clone attack, an adversary may capture a sensor node and copy the encrypted information to another node known as cloned node. Then this cloned sensor node can be installed to capture the information of the network. The adversary can also inject false information, or manipulate the information passing through cloned nodes. Continuous physical monitoring of nodes is not possible to detect potential tampering and cloning between the two victims and inject new ones.

1.4 Replay Attack

A replay attack is a form of WSN attack in which an attacker spies the conversation between the sender and receiver and valid data transmission is fraudulently repeated or delayed and takes the authenticated information. This is carried out either by the developer or by adversary who intercepts the data and retransmits it.

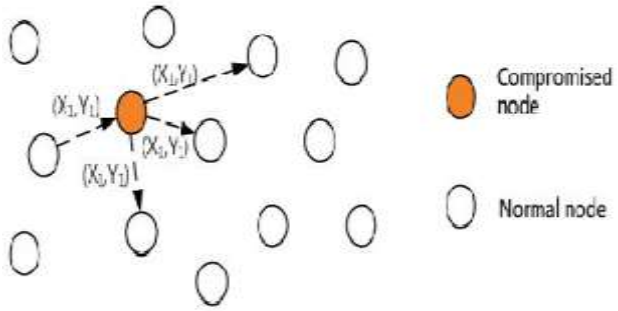

Fig 1: Replay attacks.

2. Attacks in Ad-hoc Networks

2.1 Wormhole Attack

The wormhole attack is one of the most powerful attacks presented in ad-hoc network. In wormhole attack, attacker records packets at one location in the network area and tunnels them to another location. The link that been established over wormhole link is completely under the control of the two colluding attackers. These attacks use a private, out of band channel which is invisible to wireless sensor network. Once wormhole attack is launched they can ignore the security mechanism.

2.2 Blackhole Attack

Blackhole attack tries to tend almost all the traffic towards compromised node. The attacker modifies the packets originating from some nodes and don't affect other nodes while leaving the data. The malicious node tries to attract the secure data from neighbouring nodes by advertising wrong information to make itself the original node and receives the traffic signal.

2.3 Eavesdropping

Eavesdropping is aims to obtain some confidential information that user tries kept to keep confidential during communication. The information may be private passwords, security key and location of nodes.

3. Infrastructure attacks

Infrastructure attacks are complicated and serious attacks that originate in wireless network. Spoofing attacks are main infrastructure attack in wireless network. They are main threat as they represent a form of identity compromise and facilitate a variety of traffic. The different types of spoofing attacks in wireless networks are:

3.1 DNS Spoofing

Domain name server spoofing is the technique of making a DNS entry to point to another IP than it supposed to overcome the identity of the server. DNS spoofing uses the protocol which, fails to provide the authentication for services, if authentication can't be done identities can't be verified.

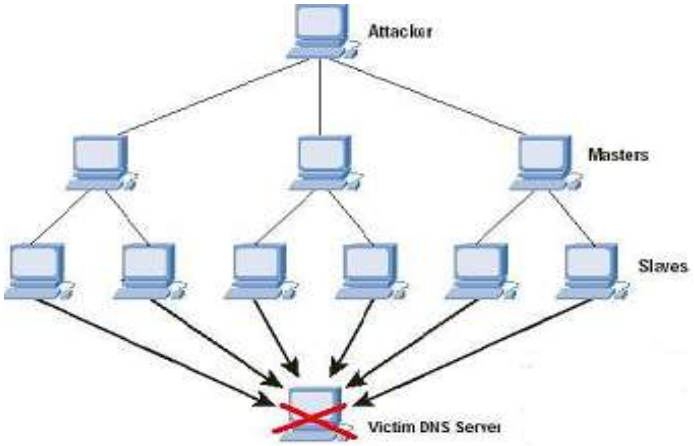

Fig 2: DNS Spoofing

3.2 Web Spoofing

Web spoofing is an interactive technique used by hackers to direct the users to visit the web site that looks like the real web site. Spoofed emails are used with spoofed web sites to build conjunction. The only difference between the spoofed and real web site is the URL.

3.3 IP Spoofing

IP spoofing refers to the creation of internet protocol packets to gain unauthorized access to computers with a forged source internet protocol address. IP address spoofing is creating IP packets using someone else's IP source address, where the intruder sends messages to a computer and shows that message coming from a trusted host.

3.4 MAC Spoofing

MAC Spoofing is a technique used by the intruder to hack into victim's computer by using the MAC address of another system by sending address resolution protocol response packet to the victim computer even though the victim did not send any request for ARP. MAC address spoofing is limited to local broadcast domain only.

III. Security Measures for Networks

Security goal for networks will depend on knowing what is there to be protected and how sensitive the data is. Therefore the security goals need to be unique for the networks. The standard goals for security are CIAA (Confidentiality, Integrity, Authentication and Availability). There are also some secondary goals present like Data Freshness, Self-Organization and Secure localization.

1. Confidentiality

It is one of the most important issues in wireless network security. It is ability to conceal the messages from an attacker so that any message communicated via the network remains confidential.

2. Integrity

To ensure the reliability of the data and ability to confirm that a message not been tampered or changed in wireless networks a key term integrity is needed between the nodes. Even if confidentiality is present in network there is still chance of poor integrity by alterations. Poor integrity cause wireless channel damage or loss of data.

VOL. 2, ISSUE 3, MARCH-2013 ISSN NO: 2319-7471

3. Authentication

Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional bogus packets. Therefore, the receiving node needs to be able to confirm that a packet received does in fact stem from the node claiming to have sent it. In other words, data authentication verifies the identity of senders. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys to compute the message authentication code (MAC).

4. Availability

Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. Since complex security measures entail a higher consumption of energy and computation power, keeping resource starved sensor networks available is challenging. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational

IV. Components in Security Requirements

The dimensions of network performance and security strength are equally important, and achieving a good trade-off between two extremes is one fundamental challenge in security design for wireless network Security never comes for free and easy. When more security features are introduced into the network, in parallel with enhanced security strength the communication, computation, and management increases overhead. Consequently, network performance, in terms of scalability, robustness, reliability, service availability and the security solutions, becomes an important concern in a resource constrained wireless network. While many contemporary proposals focus on the security reasons of their solutions from the encryption standpoint, they leave the network performance aspect largely unaddressed.

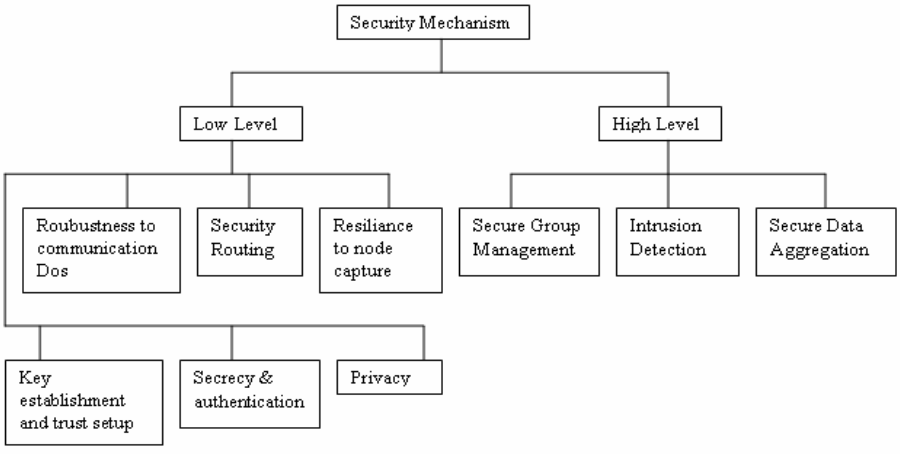

Fig 3: Security Mechanism

V. Challenges for Wireless Networks

In Wireless Sensor Networks

1. Resource Scarcity

The extreme resource limitations of sensor devices pose considerable challenges to the security mechanisms. The hardware constraints extremely necessitate the efficient security algorithms in terms of computational complexity, bandwidth and memory. This is not an easy task. Energy is the most precious resource for sensor network. Communication is especially expensive in terms of power. Clearly the security mechanisms must give special effort to be communication efficient in order to be energy efficient and being reliable to users.

2. Unreliable Communication and Transfer

The communication may be unreliable, even though the channel is reliable. This is due to the broadcast nature of the wireless sensor network. The security of the network depends heavily on the defined protocols, and these protocols depend on communication. The packet based routing of the sensor network is connectionless and thus inherently unreliable. The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus make it difficult to achieve synchronization among sensor nodes.

3. Hostile Environment

Hostile environment is a challenging situation for sensor nodes function. The possibility of destruction or capture by attackers is more. Since the nodes may be in a hostile environment, attackers can easily gain physical access to the devices. Attackers may capture a node, physically disassemble it, and extract from it valuable information (e.g. crypto graphic keys). The highly hostile environment represents a serious challenge for security researchers**.**

In Wireless Ad-hoc Networks

1. Randomized Message Forwarding

The secure Route Delegation and secure neghbor detection techniques are not sufficient to stop the immense rushing attack. A random selection technique is used to minimize the chance that a rushing adversary can dominate all returned routes. Randomized forwarding is heavily relying on the timeout to make request forward, increasing latency and reducing security. In a real network, perfect information is generally not available. Discovering the number of requests to buffer before forwarding them can adjust this parameter adaptively, based on the latency and on the parameters chosen by other nodes.

2. Secure Route Discovery

Route Discovery is composed of two stages: Route Request (RREQ) and Route Reply (RREP). Whenever a source needs to communicate to a destination and does not have a route in its Route Cache, it broadcasts a RREQ message to a route. Each neighbor receives the RREQ and appends its own address to the address list in the RREQ and re-broadcasts the packet. This process continues until either the maximum hop counter is exceeded (or RREQ is discarded) or the destination is reached. In the latter case, the destination receives the RREQ, appends its address and generates a route reply packet (RREP) back towards the source using the reverse of the accumulated route. Unlike RREQ, RREP percolates towards the source via unicast. When the source finally receives RREP, it stores the route in its Route Cache.

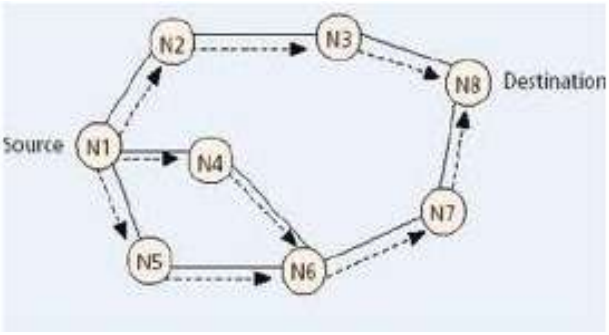

Fig 4: Secure Route discovery

In wireless Infrastructure

1. Multi-Client Environment

Multi-client environment feature is of great interest in wireless network for education, entertainment and collaborative work. Therefore concurrent multiuser interaction for networked environment, providing exchange and collection of multimedia data (images, texts, voice, sounds, video/audio streaming) is very necessary. This feature will imply the development of peer-to-peer interaction among clients and scheduling protocols to organize the priority in controlling the VR exploiting the mix of using Java and RMI.

2. Platform Independence

Platform independence is important to support different kinds of platform on which the interface could be downloaded when entering the Virtual environment, and to give the chance to visitors to use their own handheld device (which could be a Pocket PC (PPC) or a laptop, and in future a cellular phone, of any brand with different hardware capabilities). The choice of the controls and interaction features for the interface is strongly influenced by the processor, the memory, and the multimedia capabilities of the hardware. This feature provides integrity to the infrastructure in wireless networks.

3. Real Time interaction

Transmission of multimedia over wireless network is used in many applications. In order to respect network bandwidth constraints, the multimedia must be compressed for size reduction. In real-time interactive applications, low delay and high quality media are required for user satisfaction. The challenge is to find the compromise between a high compression resulting in a small size but poor quality and a low compression resulting in a rich quality but big size inducing higher delay in transmission. An adaptation scheme is proposed to manage the media compression in real-time, according to dynamical network characteristics and user context. But seems not to be very sufficient for wireless networks.

Conclusion

In summary, the major security threats for the wireless network which should be regarded as a guiding principle to come up with the challenges to the security issues in the Wireless Network are studied and analyzed. The security related features of wireless networks such as sensor networks, WMNs, ad hoc networks, wireless infrastructure are briefly discussed. Then we come up with the main challenges that are present now a days to increase the performance of the wireless networks. Therefore we have mentioned a possible strategy in detecting and protecting against wormhole attacks and maybe other attacks in infrastructure based wireless networks by focusing on identifying the WSN, AD-Hoc and infrastructure based wireless networks.

References

[1]. Verifying Physical Presence of Neighbors against Replay-based Attacks in Wireless Networks, Turgay Korkmaz, 2005.
[2]. Methodology for Securing Wireless LANs Against Wormhole Attack, V. S. Shankar Sriram, Ashish Praptap Singh and G. Sahoo, 2009.
[3]. Chaudhari H.C. and Kadam L.U, “Wireless Sensor Networks: Security, Attacks and Challenges”, 2011.
[4]. “Attacks in Wireless Networks”, 2011.
[5]. B. Dahill et al., “A Secure Protocol for Ad Hoc Networks”, IEEE ICNP, 2002.
[6]. Ian F. Akyildiz, Xudong Wang and Weilin Wang, “Wireless mesh networks: a survey,” Computer Networks, vol. 47, pp. 445-487, Jan.2005.
[7]. Divya Pal Singh, Detection of Spoofing attacks in Wireless network and their Remedies, 2012.
[8]. “Spoofing Attacks in Mobile Wireless Environments”, Proceedings of the Sixth Annual IEEE Communications Society, Secon, 2009.
[9]. Alejandro Proana, “Selective Jamming Attacks in Wireless Networks”, 2011.