Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on Security Issues in Various Wireless Networks

Amit Singla
Research Scholar,
Mewar University, Chittorgarh
Rajasthan, India

Dr. Sumeet Gill
Asstt.Professor,
Computer Science,Department of Mathematics,
M.D.U. Rohtak, India

Abstract— This paper discusses various wireless networks and their security features. Various wireless networks include wireless sensor network, mobile ADHOC network, Wi-Fi and WIMAX. The capability of each network is differed from the other. These different networks provide distinctive features of the nodes and distinct range, etc. Due to distinct features; each network has different security issues. This paper focuses on the different security features of different wireless networks. This paper also overviews basic security goals in any wireless network.

Keywords— MANET, WSN, WI-FI, WIMAX, Security

I. INTRODUCTION

Wireless networks [1,2] consist of a number of nodes which communicate with each other over a wireless channel which have various types of networks: sensor network, ad hoc mobile networks, cellular networks and satellite networks. Wireless sensor networks consist of small nodes with sensing, computation and wireless communications capabilities [1].The wireless network can be classified into two types: Infrastructured or Infrastructure less.

In Infrastructured wireless networks**,** the mobile node can move while communicating, the base stations are fixed and as the node goes out of the range of a base station, it gets into the range of another base station. The Figure: 1, given below, depicts the Infrastructured wireless network [3].

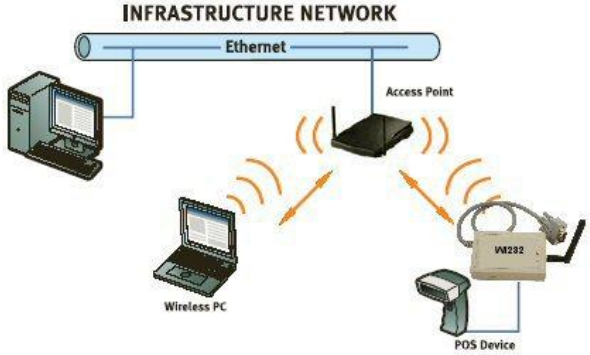

Figure 1: Infrastructured Wireless Networks

In Infrastructureless or Ad Hoc wireless network, the mobile node can move while communicating, there are no fixed base stations and all the nodes in the network act as routers. The mobile nodes in the Ad Hoc network dynamically establish routing among themselves to form their own network 'on the fly'. This type of network can be shown as in figure 2 [3].

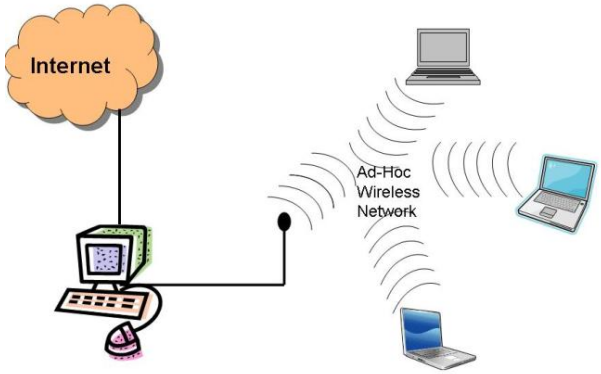

Figure 2: Infrastructureless or Ad Hoc Wireless Networks

With recent performance advancements in wireless communication technologies Security in wireless networks has recently gain a momentum and became a primary concern in attempt to provide secure communication in a hostile wireless environment. Numerous proposals were suggested without deriving a general solution. Securing a wireless network is particularly difficult for many reasons including the

1) *Vulnerability of Channels:* Message can be eavesdropped and fake messages can be injected into the network, with no necessity of physical access.
2) *Vulnerability of Nodes:* Nodes can be easily captured or stolen and can fall under the control of the attacker;
3) *Absence of Infrastructure:* Ad hoc networks operate independently of any infrastructure, which makes inapplicable any classical solutions based on certification authorities and on-line servers;
4) *Dynamically Changing Topology:* Sophisticated routing protocols designed to follow the permanent changes in topology can be attacked by incorrect routing information generated by compromised nodes, which is difficult to distinguish.[4]

II. SECURITY GOALS FOR WIRELESS NETWORK

A. Availability

Ensures survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

B. Confidentiality

Ensures certain information is never disclosed to unauthorized entities.

C. Integrity

Message being transmitted is never corrupted.

D. Authentication

Enables a node to ensure the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

E. Non-Repudiation

Ensures that the origin of a message cannot deny having sent the message.

F. Non-Impersonation

No one else can pretend to be another authorized member to learn any useful information.

G. Attacks using Fabrication

Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect [4].

III. VARIOUS WIRELESS NETWORKS

Now we are giving a brief summary on various wireless networks. These are as:

A. Wi- Max

Worldwide Interoperability for Microwave Access (WiMAX) is an emerging fixed broadband wireless technology that will deliver last mile broadband connectivity in a larger geographic area than Wi-Fi [5]. It is expected to provide coverage anywhere from one to six miles wide. Such WiMax coverage range is expected to provide fixed and nomadic wireless broadband connectivity without necessarily having a line-of-site (LOS) with a base station. WiMAX will also enable greater mobility, higher speed data applications, range and throughput than its counterpart, Wi-Fi.

WiMAX (Worldwide Interoperability for Microwave Access) provide a Point-to-Multipoint-Wireless network connectivity which operates within a range of 2 to 66 GHz [6]. Security is implemented in the so called Privacy Sub layer of the Reference Model. In the following, some essential elements of the IEEE 802.16 Security Architecture will be presented [7]. WiMAX is the emerging broadband wireless technologies based on IEEE 802.16 standards [8]. The security sub layer of the IEEE 802.16d [8] standard defines the security mechanisms for fixed and IEEE 802.16e [9] standard defines the security mechanisms for mobile network. The security sub layer supports the three things which are- (i) authenticate the user when the user enters in a network, (ii) authorize the user, if the user is provisioned by the network service provider, and then (iii) it also provide the necessary encryption support for the key transfer and data traffic. As WiMAX supports Line of Sight (LOS) and Point to Multi Point (PMP) higher frequency (10-66 GHz) to lower frequencies (2- 11 GHz) and NLOS mobile systems the security issues increased tremendously, and also, WiMAX uses radio channels which are open channels and hence pose a very serious security problem for traffic confidentiality and integrity.

B. Wimax Security Features

1) Security Association

A security association (SA) is a set of security information parameters that a BS and one or more of its client SSs share [10]. Each SA has its own identifier SAID) and also contains a cryptographic suite identifier for selected algorithms), traffic encryption keys (TEKs) and initialization vectors [11].

2) Public Key Infrastructure

WiMAX uses the Privacy and Key Management Protocol (PKM) for secure key management, transfer and exchange between mobile stations. This protocol also authenticates an SS to a BS. The PKM protocol uses X.509 digital certificates, RSA (Rivest -Shamir-Adleman) public-key algorithm and a strong encryption algorithm (Advanced Encryption Standard - AES). The initial draft version of WiMAX uses PKMv1 which is a one-way authentication method

and has a risk for Man-in-the middle (MITM) attack. To deal with this issue, in the later version (802.16e), the PKMv2 was used to provide two-way authentication mechanism.

3) *Authorization*

The authentication process is the authorization process in which SS requests for an AK and a SAID from BS by sending an Authorization Request message. This message contains SS X.509 certificate, encryption algorithms and cryptographic ID. The BS then interacts with an AAA (Authentication, Authorization and Accounting) server to validate the request from the SS, and sends back an Authorization Reply which includes the AK encrypted with the SS's public key, a lifetime key and an SAIS. WiMAX adopts the AES algorithm for encryption. "The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain-text into the final output of cipher-text. Each round consists of several processing steps, including one that depends on the encryption key. A sets of reverse rounds are applied to transform ciphertext back into the original plain-text using the same encryption key" [12]. Since DES is no more secure enough, AES is recommended in WiMAX with many supported modes: CCM-Mode and ECB-Mode (in IEEE 802.16-2004), CBC-Mode, CTRMode, AES-Key-Wrap. WiMAX has been designed carefully with security concerns but it is still vulnerable to various attacks [10].

C. Wi-Fi

Another wireless network standard, known as WiFi, is IEEE 802.11 [13]. Due to the use of un-licensed frequency bands (2.4 GHz with 14 distinct channels) in IEEE 802.11b/g, providing up to 11/54 Mbps data rate, WiFi networks have gained much attention. The initial IEEE 802.11 PHY layer includes: (i) Frequency Hopping Spread Spectrum (FHSS), (ii) Direct Sequence Spread Spectrum (DSSS), and (iii) Infrared (IR). IEEE 802.11b uses High-Rate DSSS (HR-DSSS), while IEEE 802.11g deploys OFDM.

The IEEE 802.11 MAC layer deploys the Distributed Coordination Function (DCF) as a default access technique. In this contention based scheme, WiFi STAs associated with the Access Point (AP) use their air interfaces for sensing channel availability. If the channel is idle, the source STA sends its data to the destination STA through the associated AP. If more than one STA try to access the channel simultaneously a collision occurs. The standard uses the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) mechanism to avoid collisions [14].

Point Coordination Function (PCF) is another technique that may be used in the MAC layer. In PCF, the data transmission is arbitrated in two modes: (i) centralized mode, where the AP polls each STA in a round-robin fashion, and (ii) contentionbased mode, which works similarly to DCF. In addition, the Request To Send (RTS)/Clear To Send (CTS) mechanism is applied to solve the hidden node problem [13].

D. MANETs

In the beginning, Department of Defence (DOD) did most of the research on Ad Hoc networks for their use in military applications in battlefield areas. DARPA funded a Packet Radio Network Program, which used broadcast radios for relaying data over multi hop mobile networks. Its purpose was to provide for sharing bandwidth and for operation under dynamic conditions.[15] At that time the radios were heavy and power hungry. The Survivable Radio Network (SURAN) project was sponsored by DARPA in 1980s to develop a set of mobile ad-hoc network (MANET) radio-routers, to overcome the limitations of Packet

Radio Networks. The main goals were to develop a small, lowcost, low-power radio that would support more sophisticated packet radio protocols than the DARPA Packet Radio project, develop and demonstrate algorithms that could scale to tens of thousands of nodes and develop and demonstrate techniques for robust and survivable packet networking in sophisticated electronic attacks [15].

MANET is an autonomous system of mobile nodes connected by wireless links, where communications are often achieved by multi-hop links. In a MANET, it is assumed that the nodes are free to move randomly while being able to communicate with each other without the help of existing network infrastructure, a MANET is well suited for many situations where it is not feasible to build an infrastructure for deploying a network. Some examples are battlefield communications, mobile conferencing, personal area networks, emergency services, and sensor networks. Most of work on MANET has been on routing protocol. For the comparison of routing protocols, many mobility models for MANET have been developed. However, the availability of many different mobility models without unified quantitative measure of the mobility have made it very difficult to compare the results of two independent performance studies of routing protocols [16].

E. Security Features of MANETs

1) *Availability*

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [17].

2) *Integrity*

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [18]:

- Malicious altering
- 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.

3) *Confidentiality*

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

4) *Authenticity*

Authenticity is essentially assurance that participants in communication are genuine and not impersonators [19]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations [17].

F. Wireless Sensor Network

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on [20].

G. Security in WSN

1) *Data Confidentiality*

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first [21]. In sensor networks, the confidentiality relates to the following [22]:
A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.

- In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

2) *Data Integrity*

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit [21].

3) *Data Freshness*

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness [21].

IV. CONCLUSIONS

This paper analyzes different wireless network and their security concern. The paper presents different security features of various wireless networks. Due to distinct feature of different network, each network must offer different security issues. But there are some common issues due to common security goals. That's why a common algorithm can be developed to secure these different wireless networks. .

REFERENCES

[1] Karan Singh, Rama Shankar Yadav, Ranvijay, "A REVIEW PAPER ON AD HOC NETWORK SECURITY", International Journal of Computer Science and Security, Volume (1): Issue (1).
[2] R. Shiva Kumaran, Rama Shankar Yadav, Karan Singh "Multihop wireless LAN " HIT haldia March 2007.
[3] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010, ISSN: 2010-0248.
[4] Ajay Jangra, Nitin Goel, Priyanka& Komal Bhatia, "Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture", International Journal of Electronics Engineering, 2(1), 2010, pp. 189-196.

[5] Amardeep Singh, "Trends in Broadband Wireless Networks Technologies", IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011.
[6] Awanish kumar kaushik, "A comparative study of Technical aspect of WiMAX & WiFi Netwoks Technology", ISSN: 2319-1112 /V1N3:362-370 ©IJAEEE.
[7] D. Johnston, J. Walker, "Overview of IEEE 802.16 Security," Published by IEEE Computer Society, 2004:mia.ece.uic.edu/~papers/WWW/Bubbles/segment/WiMax_Security.pdf#search=%22WiMax_Security.pdf%22.
[8] IEEE 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks —Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE Press, 2004.
[9] IEEE 802.16-2005, "IEEE Standard for Local and Metropolitan Area Networks —Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," IEEE Press, 2005.
[10] Rakesh Kumar Jha#1, Dr Upena D Dalal, "A Journey on WiMAX and its Security Issues", Vol. 1 (4) 2010, 256-263
[11] D. Park, in A Study of Packet Analysis regarding a DoS Attack in iBro Environments, vol. 8, no. 12.
[12] M. E.-H. A. E.-H. Mahmoud Narsreldin, Heba Aslan, "Wimax security," in 22nd International Conference on Advanced Information Networking and Applications, 2008, pp. 1335–1340.
[13] Navid Ghazisaidi, "Integration of WiFi and WiMAX-Mesh Networks", IEEE, 2009
[14] M. S. Kuran and T. Tugcu, "A Survey on Emerging Broadband Wireless Access Technologies," Computer Networks, vol. 51, no. 11, pp. 3013– 3046, Aug. 2007.
[15] Mahmud, Sahibzada Ali, et al. "A comparison of MANETs and WMNs: commercial feasibility of community wireless networks and MANETs."Proceedings of the 1st international conference on Access networks. ACM, 2006.
[16] Nah-Oak Song, "Wireless Networks: WLAN & MANET"http://www.mwnl.snu.ac.kr/~schoi/Courses/635-1/03-spring/Lecture_materials/03_04_28_WLAN_n_MANET.pdf
[17] Li, Wenjia, and Anupam Joshi. "Security issues in mobile ad hoc networks-a survey." Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County (2008): 1-23.
[18] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.
[19] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003
[20] Vanita Rani PG Student, Dr. Renu Dhir, " A Study of Ad-Hoc Network: A Review", Volume 3, Issue 3, March 2013.
[21] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", VOLUME 02, ISSUE 01.
[22] D. W. Carman, P. S. Krus, and B. J. Matt. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

