International Journal of Scientific & Engineering Research Volume 9, Issue 4, April-2018
ISSN 2229-5518

Study of Analysis and Wireless Network and Security

[1] N.Kavitha, [2]Selvi

Abstract — The increasing as network technologies and applications wireless networking cards to experiment with new MAC layer protocol 802.11 MAC on top of this radio subsystem wireless network virtualization enables abstraction and sharing if infrastructure and radio spectrum resources wireless network virtualization including isolation control signaling resources recovery and allocation, mobility, management. It was one of the most promising technologies for the future. Ad hoc network is a collection of wireless computer (nodes) a secure ad hoc networking routing protocol based on the design of the destination sequenced distance vector routing protocol wireless sensor in recent years. Wireless sensor networks are displayed mostly in open and unguarded environment.

Keywords— Virtualization, allocation, mobility, vector, routing protocol.

1 INTRODUCTION

Computer system researchers have a rich history of experimenting with wireless networks security. the RTS/CTS mechanism used in the 802.11 networking standard expansion of wireless services such as cellular Voice, PCS(personal communication services), mobile data and wireless LANSs .and use of WSN for data communication and processing is growing rapidly an infrastructure of WSN is built on a large number of independent sensor nodes and a base station. Wireless sensor networks are usually composed by hundreds of inexpensive, low-powered sensing device with limited memory, computational, and communication resources. Recurring them in technology forecasting efforts center around telemedicine, predictive diagnostics medical records, security, human factors, policy changes. The idea that wearable monitoring systems implemented as wireless area body networks (WBANs) offer opportunities to move beyond "telemedicine" which purports to replicate the traditional face-to-face patient/physician consultation using technology. An efficient cryptography approach for data security in WSNs using the modern encryption standard version-2 the important factors and some of the security attacks were highlighted with an overview of security solutions to establish a secure infrastructure for WSNs. This began with the following security requirements. Denial-of-service (DOS) this type of attack aims to reduce network bandwidth and paralyzed resources.

2 LITERATURE REVIEW

This section will provide the brief description and highlights using the modern encryption standard version-2 the important factors and some of the security attacks were highlighted with an overview of security solutions to establish a secure infrastructure for WSNs. This will began with the following security requirements. Denial-of-service (DOS) this type of attack aims to reduce network bandwidth and paralyzed resources the contribution, remarks and factors of the work done by researches. The security protocol was for better security using a combination of both symmetric and asymmetric cryptography algorithms. Implementing an encryption algorithm by using AES (Advanced encryption standard) has been proposed to provide for data confidentiality in a wireless sensor network. An efficient cryptography approach for data security in WSNs using the modern encryption standard version-2 the important factors and some of the security attacks were highlighted with an overview of security solutions to establish a secure infrastructure for WSNs. This began with the following security requirements. Denial-of-service (DOS) this type of attack aims to reduce network bandwidth and paralyze resources.

3 SECURITY REQUIREMENTS OF WIRELESS SENSOR NETWORKS

In wireless sensor networks, data confidentiality ensures that secrecy of sensed data is never disclosed to unauthorized parties and it is the most important issue in mission critical applications. Authors of the state that sensor node should not leak its readings to neighboring nodes. Wireless sensor networks may comprise of numerous different types of sensors like low sampling rate, seismic, magnetic, thermal, visual, infrared, radar, and acoustic, which are clever to monitor a wide range of ambient situations. Sensor nodes are used for constant sensing, event ID, event detection & local control of actuators. The applications of wireless sensor network mainly include health, military, environmental, home, & other commercial areas.

- Military Applications
- Health Applications
- Environmental Applications
- Home Applications
- Commercial Applications

- *[1]N.Kavitha, Second year MCA, Er.Perumal Manimekalai College of Engineering, Hosur, PH-9894578702. E-mail:kavithasharvesh95e@gmail.com*
- *[2]Selvi, Second year MCA, Er.Perumal Manimekalai College of Engineering, Hosur, PH-9003959015. E-mail: vselvibsc@gmail.com*

- Area monitoring
- Health care monitoring
- Environmental/Earth sensing's
- Air pollution monitoring
- Forest fire detection
- Landslide detection
- Water quality monitoring
- WSN architecture
- Characteristics
- Applications

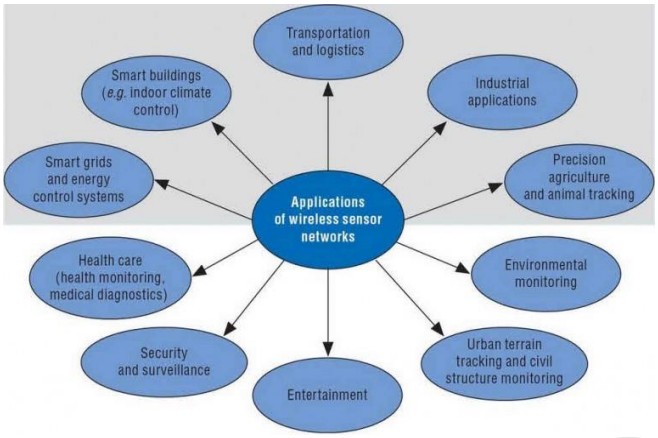


Figure 1 Wireless sensor network

We hope that you have hot a better understanding of this concept.

Thus, this is all about what is a wireless sensor network, Furthermore, any queries or to know about wireless sensor network project ideas, please give your valuable suggestions by commenting in the comment section below.

3.1 Backgrounds

This section the wireless network architectures considered in this paper. Also a discussion of the wireless protocol stack is included along with brief description of each individual protocol layer. The physical layer is further discussed

4 WIRELESS NETWORK ARCHITECTURE

The most common WSN architecture follows the OSI architecture Model. The architecture of the WSN includes five layers and three cross layers. Mostly in sensor n/w we require five layers, namely application, transport, n/w, data link & physical layer. The three cross planes are namely power management, mobility management, and task management. These layers of the WSN are used to accomplish the n/w and make the sensors work together in order to raise the complete efficiency of the network.

5 OSI (OPEN SYSTEM INTERCONNECTION)

The open system inter connection is a network reference model. It was development by ISO (international standard organization) in 1984.

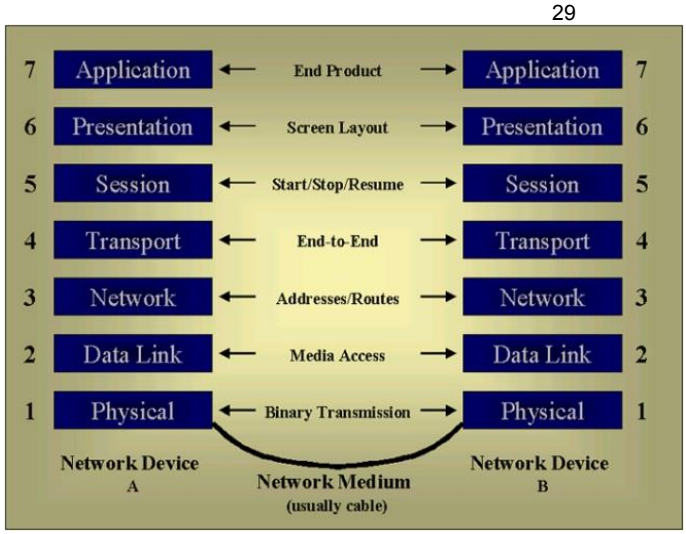


Figure 2 OSI Reference models (Open system inter connection is a network)

5.1 Uses

- It provides the primary architecture model for internet working, and communication.
- The OSI (open system inter connection) is reference model has seven layers.

5.2 Elementary of layer

The elementary of layer have a 3 type of layers. They are

- protocol specification
- Service definition
- Addressing

5.3 Service Primitives And Parameters

Primitive specifies the function to be performed. Parameter is used to pass the data and control information.

5.4 Types of Primitives

The primitive is four types is there

- Request
- Response
- Indication
- Conform

5.5 Types of layers

- Physical layer
- Data link layer
- Network layer
- Transport layer
- Session layer
- Presentation layer
- Application layer

The layers 5, 6, 7 called as an upper layer. The layers 1, 2, 3 called as a lower layer. The layers 4,5,6,7 is deals to the end-to end the data communication between the networks

5.5.1 Physical layer

The physical layer is the first layer of the Open System Interconnection Model (OSI Model). Physical layer coordinates the function, required to transmit with the bit stream over the physical medium.

5.5.1.1 Function of physical layer

- Reforestation of bits
- Data rate (or) transmission rate
- Synchronization of bits

5.5.2 Data link layer

The data link layer or layer 2 is the second layer of the seven-layer OSI model of computer networking. If provide the raw transmission facility.

5.5.2.1 Functions of data link layer

- Physical ardency
- Flow control
- Error control
- Access control
- Flaming control

5.5.3 Network layer

The network layer is the third level of the Open Systems Interconnection Model (OSI Model) it is responsible for source to destination delivery of a packet across multiple network and the layer that provides data routing paths for network communication.

5.5.3.1 Function of network layer

- Logical ardency
- Router

5.5.4 Transport layer

The transport layer is the fourth layer in the open system interconnection (OSI) model responsible for end-to-end communication over a network. It is responsible for process to delivery of the entire message.

5.5.4.1 Function of transport layer

- Connection control
- Flow control
- Error control
- Segmentation & reassembly
- Port address

5.5.5 Session layer

The session layer is the five layer of the open system inter connection (OSI). It provides the mechanism for the controlling dialogue between application and end system.

5.5.5.1 Function of session layer

- Dialogue discipline
- Grouping & recovery

5.5.6 Presentation layer

The presentation layer is the six layer of the open system inter connection (OSI) model it just provide the data and formatted the data. The presentation layer is sometimes called the syntax layer.

5.5.7 Application layer

The application layer is the seven layer of the open system inter connection (OSI) model. In the application layer uses software forget the data.

5.5.7.1 Function of application layer

- Mail server
- File transfer & access
- Remote login
- Access by the www

6 NEEDS OF WIRELESS SECURITY

Security is one of important challenge which is to be handled in the area of wireless technology these days. Current security standards have shown that security is not keeping up with the growing use of wireless technology. Every now and then a new vulnerability comes in existence to the existing wireless standards. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed.the ability to enter a network while mobile has great benefits.

7 SECURITY REQUIREMENTS

While any organization wants to product its sensitive data, to detect tampering of data and to limit access to authorized individuals, various industries must also comply with an array of regulatory and industry requirements and guidelines. One common requirement is that sensitive data that is stored or communicated over public networks must be encrypted using certified algorithms. The web was designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication.

8 SECURITY THREATS TO WIRELESS NETWORK

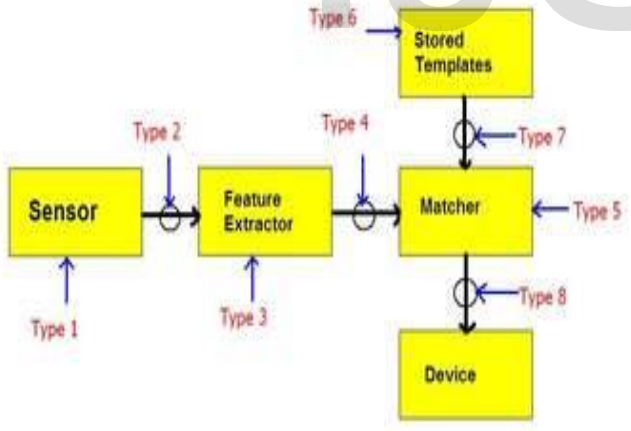
Protection of wireless networks means production from attacks on confidentiality, integrity and availability possible threats come from vulnerabilities in the security protocols. This section explains various types of security attack techniques attacks.

8.1 Difference types of security attacks

- Traffic analysis
- Eavesdropping
- Unauthorized access
- Denial of services(DOS)
- Dictionary-building attackers

8.1.1 Traffic analysis

Traffic analysis is a special type of inference attack technique that looks at communication patterns between entities in a system. "Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security.



8.1.2 Unauthorized access

The unauthorized access is when someone gains access to a website, program, server, service, or other system using.of the most important research areas within wireless communication. Recent advance in micro electro mechanical system and low power highly integrated digital electronics have led to the development of micro sensors.

8.1.3 Denial-of-services

Accessing the service In a DOS attack, the attacker usually sends excessive message asking the network or server to authenticate requests that have invalid return address.

8.1.4 Dictionary-building attacks

A dictionary attacks is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a Password.

9 CONCLUSION

As wireless services continue to add more capabilities such as multimedia and QOs, low power design remains one of the most important research areas within wireless communication. Recent advance in micro electro mechanical system and low power highly integrated digital electronics have led to the development of micro sensors. A denial-of-services (DOS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from. Multimedia and QOs, low power design remains one of the most important research areas within wireless communication. Recent advance in micro electro mechanical system and low power highly integrated digital electronics have led to the development of micro sensors.

REFERENCES

[1] Christine E. Jones, Krishna M. Sivalingam Prathima Agrawal And Jyh Cheng Chen,"A Survey of Energy Efficient Network Protocols for Wireless Networks Wireless Networks 7, 343–358, 2001

[2] Kemal Akkaya *, Mohamed Younis"A survey on routing protocols for wireless sensor networks accepted 1 September 2003

[3] Steve Warren1, Jeffrey Lebak1, Jianchu Yao3, Jonathan Creekmore2, Aleksandar Milenkovic2, and vanov2 Emil Jo Interoperability and Security in Wireless Body Area Network Infrastructures

[4] Suat Ozdemir a,*, Yang Xiao b Secure data aggregation in wireless sensor networks: A comprehensive overview _ 2009 Elsevier B.V. All rights reserved.

[5] Michael Neufeld, Jeff Fifield, Christian Doerr, Anmol Sheth and Dirk Grunwald SoftMAC – Flexible Wireless Research Platform.

[6] Yih-Chun Hu a,*, David B. Johnson b, Adrian Perrig a "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks".

[7].Xin Wang, Prashant Krishnamurthy, and David Tipper
Wireless Network Virtualization Journal of Communications Vol. 8, No. 5, May 2013.

[8] Shio Kumar Singh 1, M P Singh 2, and D K Singh 3 Energy Efficient Homogenous Clustering Algorithm for Wireless Sensor Networks Vol.2, No.3, August 2010

[9] Vivek Srivastava*, James Neel*, Allen B. MacKenzie*, Rekha Menon*, Luiz A. DaSilva*, James E. Hicks*, Jeffrey H. Reed*, Robert P. Gilles** Using Game Theory to Analyze Wireless Ad Hoc Networks Wireless Ad Hoc Networks".

1[0] Arunesh Mishra, Nick L. Petroni, Jr.*,y, William A. Arbaugh and Timothy Fraser Security issues in IEEE 802.11 wireless local area Networks: a survey.