IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, Sept 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Secure and Authenticated Source Routing in Wireless Networks

Dhiraj Khurana[1], Mukesh Singla[2]

[1]Assistant Professor, UIET, MDU, Rohtak (India)

[2]Associate Professor, VCE, Rohtak (India)

Abstract

Wireless networking is today's glamour technology. We can hardly pick up a technology publication without encountering articles extolling its virtues or excoriating its faults. Wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling. If a user, application or company wishes to make data portable, mobile and accessible then wireless networking is the answer. A wireless networking system would rid of the downtime you would normally have in a wired network due to cable problems. It would also save time and money due to the fact that you would spare the expense of installing a lot of cables. Also, if a client computer needs to relocate to another part of the office then all you need to do is move the machine with the wireless network card [1].

Keywords: Protocols, WSN, Duplicate, Webpage, Prioritization

1. Introduction

Wireless Sensor Network (WSN) can be defined as the network of autonomous sensors which cooperatively monitor physical or environmental conditions such as temperature, pressure, sound or vibration [11]. In other words, wireless sensor network is composed by a large number of nodes with processing, sensing and radio communication capabilities, scattered throughout a certain geographical region where the sensory data is routed in a multi hop ad hoc fashion from the originator sensor node to a remote control station. WSN are the subclass of ad hoc network wherein group of sensors capable of making measurements exchange information with each other.

Over recent years, the market for wireless communications has experienced incredible growth. Wireless technologies have quickly found a significant place and popularity in business and the computer industry. Their major motivation and benefit is increased flexibility and mobility.

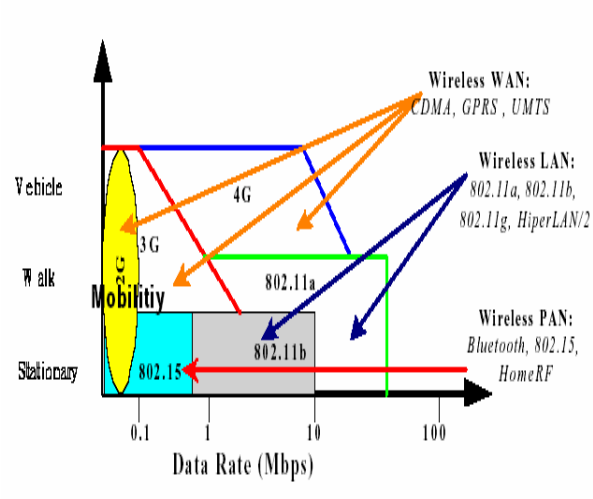

Figure 1: Overview of Wireless Networks

This figure 1 illustrates the three main categories of wireless networks and their coverage ranges. The most successful wireless networking technology this far has been 802.11and hence is the main focus of this research [2].

2. IEEE 802.11 Wireless Standards:

2.1 History of 802.11

The IEEE breaks their standards into various committees. The IEEE 802 Committee deals with Local and Metropolitan Area Networks. The 802 series of standards is broken into 7 working groups that focus on specific issues within the overall discipline of LANs and MANs [6].

The following is a list of some of the 802 working groups:

- 802.1: Bridging and Management

- 802.2: Logical Link Control
- 802.3: CSMA/CD Access Method
- 802.4: Token-Passing Bus Access Method
- 802.7: Broadband LAN
- 802.11: Wireless

2.2 Wireless Local Area Networks

The IEEE 802.11 wireless LAN technology has followed the trend of most computing technologies over the past 20 years, and expanded exponentially. A WLAN is analogous to a wired LAN but radio waves being the transport medium instead of traditional wired structures. This allows the users to move around in a limited area while being still connected to the network. Thus, WLANs combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs [2]. In other words WLANs provide all the functionality of wired LANs, but without the physical constraints of the wire itself.

2.2.1 Working of WLANs

Moving data through a wireless network involves three separate elements: the radio signals, the data format, and the network structure. Each of these elements is independent of the other two, so you must define all three when you invent a new network. In terms of the OSI reference model, the radio signal operates at the physical layer, and the data format controls several of the higher layers. The network structure includes the wireless network interface adapters and base stations that send and receive the radio signals. In a wireless network, the network interface adapters in each computer and base station convert digital data to radio signals, which they transmit to other devices on the same network, and they receive and convert incoming radio signals from other network elements back to digital data. Each of the broadband wireless data services use a different combination of radio signals, data formats, and network structure. We'll describe each type of wireless data network in more detail later in this chapter, but first, it's valuable to understand some general principles.

2.2.2 Security Features of Wireless LANs

A message traveling by air can be intercepted without physical access to the wiring of an organization. Any person, sitting in the vicinity of a WLAN with a transceiver with a capability to listen/talk, can pose a threat. Unfortunately, the same hardware that is used for WLAN communication can be employed for such attacks. To make the WLANs reliable the following security goals were considered:

- Confidentiality
- Data Integrity
- Access Control

3. Problem Definition

A secure communication is always the major requirement of a network. In case of wireless network, as open network the secure transmission is the major requirement. Because of this lot of work is already done in this area still there are some flaws always in security. We have also concerning to the same problem in the proposed system. In this proposed system we are defining the authentication based routing. The cryptography based routing decision is being taken place in this proposed system. We representing a third party scheme that will deal will both the routing decision as well as with the security. This work will work as the interfacing between the host and the ISP. We will set a series of such hops that will work as the layers between the two ends of data communication. The proposed system is basically works for a wan network to enhance the security over the web.

4. Existing Work

This part of paper seeks to review the existing literature for the purpose to define the problem precisely and crystallize its objectives. This not only helps in setting the direction for the research but also broadens the mental horizon and the vision of its implications.

4.1 Secure Source Route

In paper [6], author proposes a novel approach to enhance data confidentiality when transmitting across the insecure networks.
Paper [7], describes policy engine and secure source routing. In today's Internet, inter-domain route

control remains elusive; nevertheless, such control could improve the performance, reliability, and utility of the network for end users and ISPs alike.

4.1.1 Secure Source Route for Mobile Ad hoc Networks

Paper [9], gives brief introduction of Network routing in wireless ad hoc networks, how it is liable to attacks that may have a grave impact on network operations.
Author, in paper [10] discuss about Mobile Ad hoc Networks (MANETs) that are open to a wide range of attacks due to their unique characteristics such as dynamic topology, open medium, absence of infrastructure, multi hop scenario and resource constraint.
In paper [5], a formal model tailored to the security analysis of on demand source routing protocols in MANET, and a new routing protocol, called ENDAIRA, was proven secure in the model.
Paper [9], represent about a comparative study for secure routing in MANET and comparison between different types of protocols.

4.1.2 Secure Source Route for Wireless Sensor Networks

Paper [9], represent about Secure and Energy Aware Routing (SEAR) in Wireless Sensor Networks. Lifetime optimization and security are two important design issues for multi-hop wireless sensor networks with non-replenish able energy resources.
Paper[8], discuss about the Several routing protocols have been proposed in recent years for possible deployment of Mobile Ad hoc Networks (MANETs) in military, government and commercial applications.

5. Proposed Architecture for secure and authenticated source routing:

In this proposed system is defined which works for the authentication based routing protocol. It is cryptography based authentic and secure routing protocol, which is basically implemented using four modules. This protocol use DNS Server, ISP, Host Sender, Host Receiver and Policy-Engine. They all communicate with each other via policy-engine as shown in figure 2:

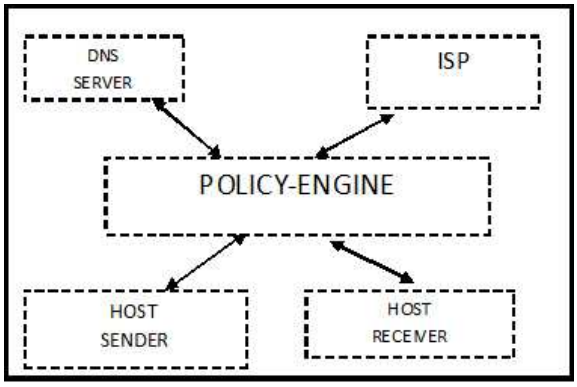

Figure 2: Architecture of proposed system

6. Module Description

6.1 Forwarding and Stamping

In first module of proposed system i.e. forwarding transfer of packets from source node to destination node takes place in a network via some intermediate nodes. Forwarding can be done by different techniques that are (i) Unicast type, (ii) Broadcast type, (iii) Multicast type. All these techniques differ in number of destination hosts which get sent packets form the source host.
In this module stamping is also take place with forwarding. Stamping is used to add security feature along with forwarding process. First of all a packet at the sender's end is checked for security. If it is found secure only then it is relayed from host sender to receiver. Whenever a packet is stamped secure by host sender, then only it is forwarded to the receiver. Stamping is done at each node. At host receiver every packet is checked whether it is stamped secure or not if it is secured then only it is accepted by the host receiver. Thus stamping provides security with the help of handshaking.
In this manner proposed system works with two techniques i.e. forwarding and stamping simultaneously. Forwarding of a packet takes place only if stamping over packets done successfully.

6.2 Distribution of Delegated Capabilities

In the proposed system, host sender sends packets to receiver host. It also request for packets and all these requests are collected by DNS (Domain Name System) server. DNS is a technology which is used to manage the names of websites and other internet domains. DNS facilitates us by allowing to type names of website into address bar of web browser

and automatically generates the address on the internet corresponding to given name.

6.3 Policy

Policy exists at the end user i.e. at host sender. If host sender wants to communicate with the host receiver, it doesn't communicate directly with it. It uses policy-engine for such communication; here policy-engine works as an intermediate as it works for distribution of delegated capabilities. Thus policy feature of the proposed system i.e. communication between host sender and host receiver does not take place in a single step.

6.4 Protocol Interactions

Final module of proposed system is Protocol Interaction. Protocols are the rules obeyed by nodes to communicate in a network. Protocols are also necessary for security purpose. In the proposed system two protocols are used to implement the system. First one is ICMP and second one BGP.
ICMP is Internet Control Message Protocol. It is one of the core protocols of IP (Internet Protocol) suite. Main function of ICMP is to send error messages. These error messages are sent under certain conditions like, when a requested service is not available or when a host or router could not be reached on time.
In the proposed system ICMP is used to enhance the security feature. Here an ICMP error message is the time to live (TTL) exceeded message. Each node or machine between host sender and receiver, which forward the data packet, called datagram, has to decrement Time-To-Live field of the IP header by one. If the TTL filed of the header reaches 0 before reaching the host receiver, then came the function of ICMP message. In this situation an ICMP message showing Time to live exceeded, is sent to the host sender (source of datagram).

7. Results

The implementation works DNS Server, ISP, Host Sender, Host Receiver and Policy-Engine installed. These four network components are established in LAN and among them one is considered as Policy-Engine and other are legitimate hosts which detect that unauthorized user on the basis of sent packets.
The screen shots of proposed system are shown, which indicates different modes of IDS monitor such as (i) Source Host, (ii) Policy-Engine and (iii) Source Receiver.

7.1 Source Host

If we want to communicate source host with source receiver than firstly establish the connection, whenever connection has been established then host source will ready to send packets, once the connection has been established then the packets will ready to send as shown in fig 3.Now in next step Fig 4 shows to select the source file which we want to transfer. In this step the source path of the file is text box shown in the Fig 5. There are number of files are open when we select the open button. Now it asks to enter the file name and files of type.

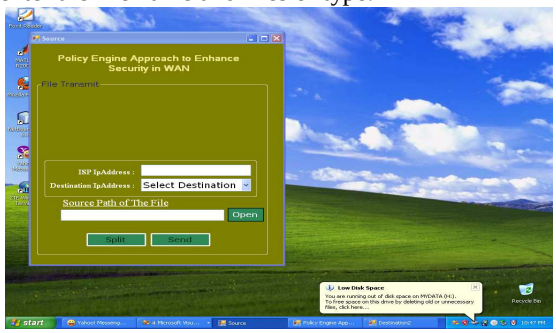

Fig 3 Source Host Ready to Send Packets

Once File name has been selected then go to select the Open button Once choose open button then appear a dialog box which consist Source Path of the file and at last file name place to the selected path.

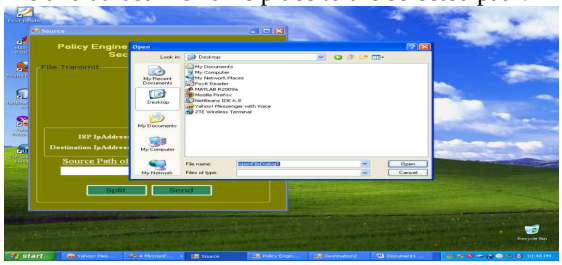

Fig 4 Select the Source File to Transfer

Once Source path of the file selected then go to next step. Now next step shows a dialog box which shows Source Machine with Specified ISP and Destination Host. In this specified ISP address has been selected and destination IP address. In this step, it provides an approach to enhance security in wireless network.
There are number of different techniques can be used that are (i) unicast type, (ii) broadcast type, (iii) multicast type. All these techniques differ in number of destination hosts which get sent packets form the source host.

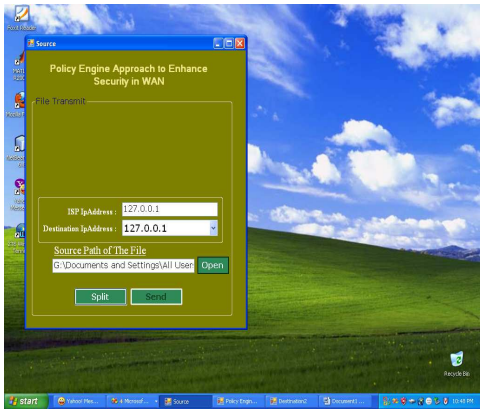

Fig 5 Source Machine with Specified ISP and Destination Host

7.2 Policy-Engine

If host source wants to communicate with the host receiver, it doesn't communicate directly with it. It uses policy-engine for such communication; here policy-engine works as an intermediate as it works for distribution of delegated capabilities. Thus policy feature of the proposed system i.e. communication between host sender and host receiver does not take place in a single step. This work takes places in following 2 step processes.
Step 1: Source host communicate with Policy-Engine by RC1.
Step 2: Policy-Engine communicate with host reciver by RC2.

Fig 6 Policy Engine

7.3 Source Receiver

At receiving end, there are number of destinations available to get the packets in which sent by the host source. Firstly, Source host ready to send packets and go to next step. Now select the source file to transfer in which we want to send packets. At last select the destination address where we want to transfer packets.

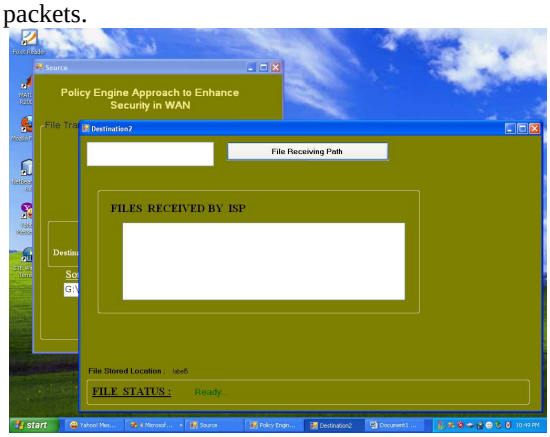

Fig 7 Receiver End

Once received the packets by the receiver then it will go to the last step. Now last step, indicates that select destination to Place files in which store the files. In this final step dialog box shows to select the location where we place the files by Destination.

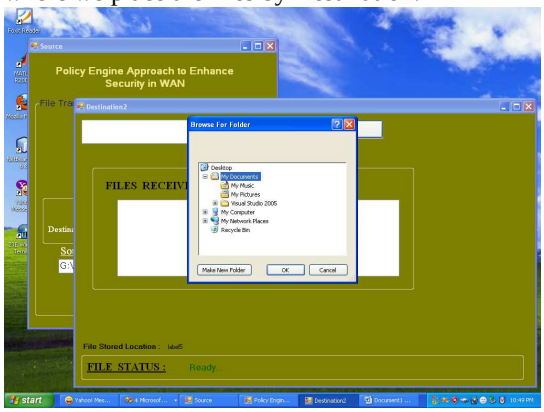

Fig 8 Select Destination to Place File

8. Conclusion

The proposed system will provide the security aspects in case of WAN network. The system will work as the intermediated between each data transmission over the network. The system will provide a handshaking mode of the security. It means the security policy will be attached on both sides of the transmission i.e. on sender and receiver side. The cryptographic security is implemented as the intermediated. Other then this policy engine will work as the intermediated service provider for different servers including ISP, DNS and Web Server etc.

References

[1] Introduction "Windows Networking" http://www.windowsnetworking.com/articles_tutorials/introduction-wireless-networking-part1.html
[2] Nilufar Baghaei, "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients", Honors Project Report, 2003
[3] Karygiannis, T., & L. Owens. (2002). Draft:" Wireless Network Security - 802.11, Bluetooth and Handheld Devices". USA. National Institute of Standards and Technology
[4] Hannikainen, M., T. D. Damalainen, M. Niemi, & J. Saarinen. (2002). "Trends in Personal Wireless Data Communications". Computer Communications, 25 Elsevier. Page(s): 84-99.
[5] Jean-Paul Saindon, "Techniques to resolve 802.11 and wireless LAN technology in outdoor environments", News Article at SecurityMagazine.com, Aug 08 2002.
[6] Gast, M. (2002). Chapter 2: Overview of 802.11 Networks, 802.11 Wireless Networks: The Definitive Guide. O'Reilly ISBN 0-596-00183-5. April.
[7] Stallings, W. (2001). IEEE 802.11: moving closer to practical wireless LANs. IT Professional. Volume: 3 Issue: 3. Page(s): 17 –23. June.
[8] IEEE Std. 802.11a (1999). Supplement to ANSI/IEEE. Std 802.11, 1999 Edition. Part 11: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications": Higher Speed Physical Layer (PHY) in the 5 GHz band. IEEE, Inc.
[9] IEEE Std. 802.11b (1999). Supplement to ANSI/IEEE. Std 802.11, 1999 Edition. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band. IEEE, Inc. ISBN 0-7381-1811-7. September
[10] G. Held, "Securing Wireless LANs", John Wiley & Sons Ltd, 2003, chapter 5, pp. 113-148.
[11] Chris Townsend and Steven Arms, "Wireless Sensor Networks: Principles and Applications" chapter-22, Micro-Strain Inc., pp. 439-449, 2004.