STUDY OF VARIOUS NETWORK TYPE SECURITY PROTOCOLS

Sudhakar Singh[1], P.K. Khare[2], Prashant Mor[3]

[1] Research Scholar, [2] Professor and Head, [3] Scientific Officer,

Department of Physics and Electronic, RDVV, Jabalpur (M.P.),(India)

ABSTRACT

In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities. Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols at each layer in the telecommunication exchange that both ends of the exchange must recognize and observe. In recent years, wireless networks have gained rapid popularity. Wireless networks are inexpensive and provides mobility but they are prone to a variety of threats like denial of service, replay attacks, eavesdropping and data modification. A security protocol or cryptographic protocol or encryption protocol is an abstract or concrete protocol that performs a security related function and applies cryptographic methods, often as sequences of cryptographic primitives. A protocol describes how the algorithms should be used. A sufficiently detailed protocol includes details about data structures and representations at which point it can be used to implement multiple, interoperable versions of a program. Cryptographic protocols are widely used for secure application level data transport. This paper presents the various network types and its related security protocols architecture and applications.

Keywords- TCP/IP, Wi-Fi, Bluetooth, Sensor Network, SPINS

I. INTRODUCTION

The Internet protocols are the world's most popular open-system protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications. The Internet protocols consist of a suite of communication protocols of which the two best known are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The Internet protocol suite not only includes lower layer protocols (such as TCP and IP), but it also specifies common applications such as electronic mail, terminal emulation and file transfer. Internet protocols were first developed in the mid 1970s, when the Defense Advanced Research Projects Agency (DARPA) became interested in establishing a packet switched network that would facilitate communication between dissimilar computer systems at research institutions. With the goal of heterogeneous connectivity in mind, DARPA funded research by Stanford University and Bolt, Beranek and Newman (BBN). The result of this development effort was the Internet protocol suite, completed in the late 1970s. TCP/IP later was included with Berkeley Software Distribution (BSD) UNIX and has since become the foundation on which the Internet and the World Wide Web (WWW) are based**[1]**.

When computers talk over the Internet, the language they speak is the TCP/IP. It is also the protocol of choice for most medium and large-sized networks. Novell Netware, UNIX and Window NT networks can all implement TCP/IP, particularly on growing networks and on ones that use client/server or web-based applications. TCP/IP is one of the oldest protocols and is proven technology that is used by millions of computer users around the globe. Its broad acceptance, reliable history and extensive capabilities make it a good choice for most LAN-to-WAN installations. The TCP/IP protocol suite, used in the Internet, was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not match exactly with those in the OSI model. The TCP/IP protocol suite is made of five layers.

- Application layer
- Transport layer
- Internet layer
- Network access layer
- Physical layer

The first four layers provide physical standards, network interface, Internet working and transport functions that correspond to the first four layers of the OSI model. The three top most layers in OSI model however are represented in TCP/IP by a single layer called the application layer Figure 1**[1-2]**. A number of applications have been standardized to operate on top of TCP. We define three of the most common here.

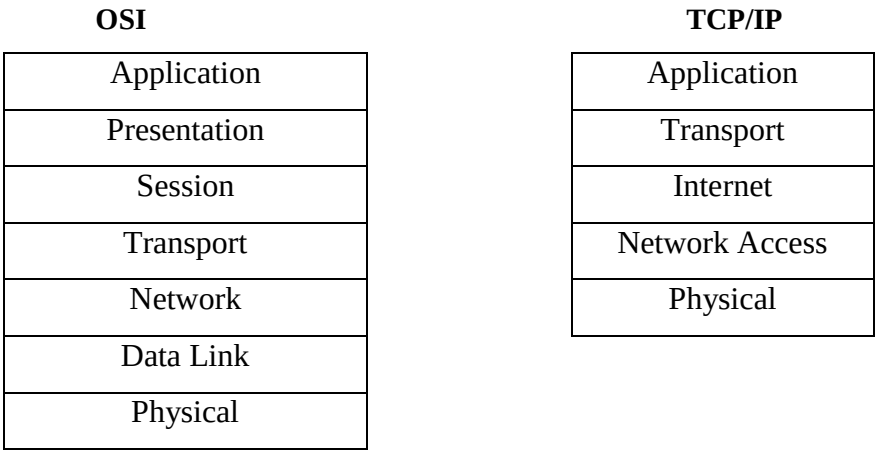


Figure 1: Comparison of OSI and TCP/IP Model

1.3 Simple Mail Transfer Protocol (Smtp)

SMTP provides a basic electronic mail facility. It provides a mechanism for transferring messages among separate hosts. Features of SMTP include mailing lists, return receipts and forwarding. Once a message is created, SMTP accepts the message and makes use of TCP to send it to an SMTP module on another host. The target SMTP module will make use of local electronic mail package to store the incoming message in user's mailbox.

1.2 File Transfer Protocol (Ftp)

FTP is used to send files from one system to another under user command. Both text and binary files are accommodated and the protocol provides features for controlling user access. When a user wishes to engage in file transfer, FTP sets up a TCP connection to the target system for the exchange of control messages. This connection allows user ID and password to be transmitted and allows the user a file transfer is approved a second TCP connection is set-up for the data transfer. The file is transferred over the data connection, without

the overhead of any headers of control information at the application level. When the transfer is complete, the control connection is used to single the completion and to accept new file transfer commands.

1.3 Telnet (Terminal Network)

The main task of the Internet and its TCP/IP protocol suite is to provide services for users. For example, users want to be able to run different application programs at a remote site and create results that can be transferred to their local site. One way to satisfy these demands is to create different client-server application programs for each desired service. Program such as file transfer programs (FTP), e-mail (SMTP) and so on are already available. But it would be impossible to write a specific client-server program for each demand.

The better solution is a general purpose client-server program that lets user access any application program on a remote computer, in other words, allow the user to log on to a remote computer. After logging on, a user can use the services available on the remote computer and transfer the results back to the local computer. TELNET is an abbreviation of Terminal Network. Client-server application program is called TELNET.

II. SECUTITY PROTOCOLS

Security is becoming more and more crucial as the volume of data being exchanged on the Internet increases. Various protocols have been developed to measure security, which can be applied to the application layer and IP layer.

2.1 Secure Socket Layer

Secure sockets Layer (SSL) is the Internet security protocol for point-to-point connection. With the growth of the Internet, many applications need to securely transmit data to remote applications and computers. SSL was designed to solve this problem. Many popular web browsers like Netscape communication and Internet Explorer use SSL to protect again eavesdropping, tampering, and forgery. In SSL, when clients and servers make connections they authenticate each other. Once authenticated a "secure pipe" is established and data can be securely exchanged as shown in Figure 2**[1-3]**. SSL uses the strong encryption technologies from RSA Data Security. Some practical application of SSL is.

- Client/Server systems: Securing database access
- Financial: Remote banking programs
- Information systems: Remote access and administration application
- Travel industry: Create online reservation systems and secure information transfer

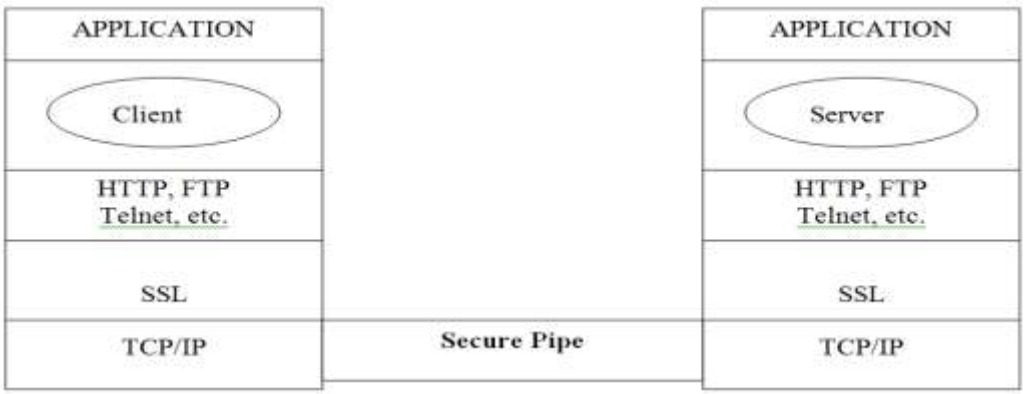
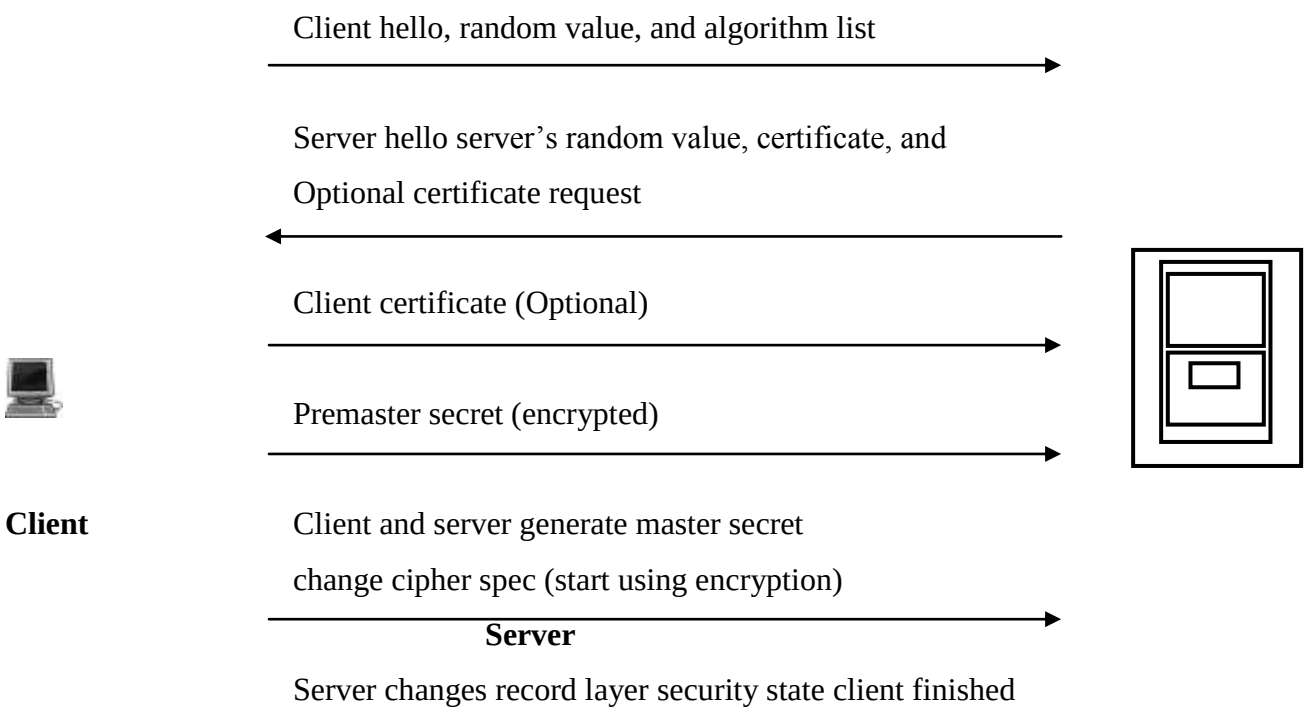


Figure: 2 Secure Socket Layer

2.2 Transport Layer Security

The IETF established the TLS working group in 1996 to develop a standard transport security protocol. The working group began with SSL version 3, as its basis and released RFC 2246, TLS protocol version 1.0 in 1999 as a proposed standard. The working group also published RFC 2712, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)" as a proposed standard, and two RFCs on the use of TLS with HITP. Like its predecessor, TLS is a protocol that ensures privacy between communicating applications and their uses on Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message**.** Transport Layer Security (TLS) is composed of two parts. The TLS Record Protocol and the TLS Handshake protocol. The TLS Record Protocol provides connection security by using supported encryption methods, such as the data encryption standard (DES). The TLS Record protocol can also be used without encryption. The TLS Handshake protocol allows the server and the client to authenticate each other and to negotiate a session encryption algorithm and cryptographic keys before data is exchanged.

Though TLS is based on SSL and is sometimes referred to as SSL, They are not interoperable. However, the TLS protocol does contain a mechanism that allows a TLS implementation to back down to SSL 3.0. The difference between the two is in the way they perform key expansion and message authentication computation. TLS uses the MD5 and SHA (Secure Hash Algorithm) algorithms together to determine the session key. Though SSL also uses both hashing algorithms, SSL is considered less secure because the way it uses them forces a reliance on MD5 rather than SHA. The TLS Record Protocol is a layered protocol. At each layer, message may include fields for length, description and content. The record protocol takes messages to be transmitted, fragments the data into manageable blocks, optionally compressed the data, applied a message authentication code (MAC) to the data, encrypt it and transmits the result. Received data decrypted verified, decompressed and reassembled and then delivered to higher-level clients. The TLS Handshake protocol involves the following steps, which are summarized in Figure 3**[1-2,5]**.



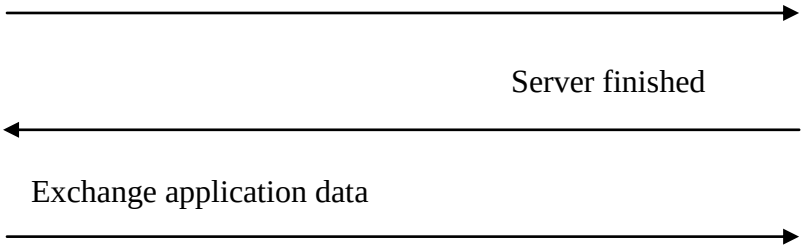


Figure 3: TLS Handshake Protocol

Step 1: Exchange hello messages to agree on algorithms, exchange random values and check for session resumption.

Step 2: Exchange the necessary cryptographic parameters to allow the client and server to agree on a per-master secret.

Step 3: Exchange certificates and cryptographic information to allow the client and server to authenticate them selves.

Step 4: Generate a master secret from the premaster secret and exchanged random values.

Step 5: Provide security parameters to the record layer.

Step 6: Allow the client and server to verify that their peer has calculated the same security parameters and that the handshake occurred without tempering by an attacker.

Though it has been designed to minimize this risk, TLS still has potential vulnerabilities to a man in the middle attack. A highly-spilled and well-placed attacker can force TLS to operate at lower security levels. Regardless, through the use of validated and trusted certificates, a secure cipher suit can be selected for the exchange of data. Once established, a TLS session remains active as long as data is being exchanged. If sufficient inactive time has elapsed for the secure connection to time out, it can be reinitiated.

2.3 IPsec

Internet protocol security (IPSec), a set of protocols developed by the Internet Engineering Task Force (IETF) for encryption and authentication of TCP/IP traffic, is the leading standard for cryptographically-based authentication, integrity and privacy services. At the IP layer, computers on a network communicate by routing datagram packets that contain data, destination addresses, source addresses and other information. In a corporate LAN or the Internet where packet datagram's are transmitted "as is" unencrypted a corporate attacker could hijack, forge or modify them. IPSec secures the network packets to create a secure network of computers over insecure channels. It enables users to communicate securely with a remote hast over the Internet via VPNs. Where SSL authentication and encrypts communication between clients and servers at the application layers, IPSec secures the underlying network layers. IPSec provides the capability to secure communication across a LAN, across private and public WAN's and across the Internet. Some practical applications of IPSec are.

(i) A company can build a secure virtual private network over the internet or over a public WAN. This enables a business to rely heavily on the internet and reduce its need for private networks, saving costs and network management overhead.

(ii) An end user whose system is equipped with IP security protocols can make a local call to an internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecomputers.

(iii) IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

The principle feature of IPSec that enables it to support these varied applications is that I can encrypt and/or authenticate all traffic at the IP level. Thus all distributed applications, including remote login, client/server, email, file transfer, web access and so on, can secured. Following are benefits of IPSec **[1]**:

(i) When IPSec is implemented is a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

(ii) IPSec in a firewall is a resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the internet into the organization.

(iii) IPSec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router. Even if IPSec is implemented in end systems, upper-layer software, including applications is not affected.

(iv) IPSec can be transparent to the end users. There is no need to train users on security mechanisms issue keying material on a per user basis, or revoke keying material when users leave the organization.

(v) IPSec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual sub network within an organization for sensitive applications.

IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s) and put in place any cryptographic keys required to provide the requested services. Two protocols are used to provide security: an authentication protocol designed by the header of the protocol, Authentication Header (AH); and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP). The services are provided by the AH and ESP protocol which are shown in Table1**[1,4]**.

Table 1: IPSec services

Services	AH	ESP (Encryption Only)	ESP (Encryption plus Authentication)
Access control	√	√	√
Connectionless integrity	√		√
Data origin authentication	√		√
Rejection of replayed packets	√	√	√
Confidentiality (encryption)		√	√
Limited traffic flow confidentiality		√	√

A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA). In any IP packet, the security association is uniquely identified by the destination address in the IPv 4 or IPv 6 header.

2.4 Authentication Header (Ah)

The Authentication Header provides connectionless integrity and data origin authentication for IP datagram's. It also optionally provides protection against replays. The AH header is shown in figure 4**[1,5]**. It is either follows the IPv4 header or is an IPv6 extension header, depending on which version of IP it is used with.

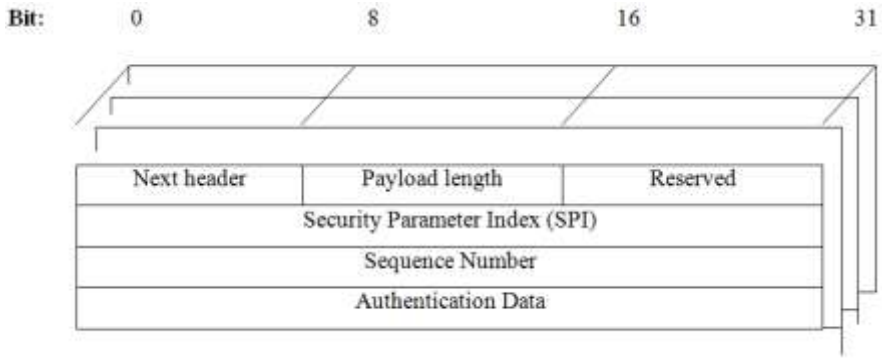


Figure 4 IPSec Authentication Header

The next header field identifies the type of the next payload after the Authentication Header. The payload length field specifies the length of the AH in 32-bit words (4-byte units), minus 2. The reserved field is reserved for future use; it is set to zero for now. The security parameter index (SPI) field is an arbitrary 32-bit value that, in combination with the destination IP address, uniquely identifies the security association for this datagram. The sequence number field contains a monotonically increasing counter or sequence number. This field is used to protect against replay, but it is present even if the receiver does not elect to enable the anti replay service for a specific SA (Security Association). The sender counter and the receiver's counter are initialized to 0 when an SA is established. If anti replay is enabled, which is the default, the transmitted sequence number must never be allowed to cycle. Thus the sender's counter and the receiver's counter must be reset by establishing a new SA and thus a new key prior to transmitting the $2^{32\ nd}$ packet on an SA. Finally, Authentication Data is a variable length field that contains the message integrity code for this packet. The field must be an integral multiple of 32 bits in length. All does not prescribe a specific message digest algorithm. DES and MD5 among others can be used.

2.5 Encapsulation Security Payload (Esp)

The Encapsulating security payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentially. As an optional feature, ESP can also provide the same authentication services as AH. ESP header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, or in combination with AH. The ESP header is inserted after the IP header and before the upper-layer protocol header (when used between a pairs of hosts) or before an encapsulated IP header when used to tunnel between a pair of security gateways. Like AH, the ESP header either follows the IPv4 header or is an IPv6 extension header. Its format is shown in Figure 5**[1-4]**. The security parameter index (SPI) field has the same function as in the AH. It helps the receiving host identify the security association to which the packet belongs.

Similarly, the sequence number field protects against replay attacks. The packets payload Data contains the data described by the next header field. If confidentiality is selected, then the data is encrypted by whatever encryption algorithm was associated with the security Association. Padding is sometimes necessary, for

example, because the encryption algorithm requires the plaintext to be a multiple of some number of bytes or to ensure that the resulting cipher text terminates on a 4-bytes boundary. The pad length field records how much padding was added to the data. Finally, the Authentication Data Carrier Variable Field (must be an integral number of 32-bit words) that contains the integrity check value computed over the ESP packet minus the Authentication Data Field.

One of the most popular ways to use the ESP is to build an "IPSec tunnel" between two routers. For example, a corporation wanting to link two sites using the Internet could configure a tunnel from a router at one site to a router at the other site. This tunnel may also be configured to use the ESP with confidentiality and authentication, thus preventing unauthorized access to the data that traverses this virtual link and ensuring that no spurious data is received at the far end of the tunnel.

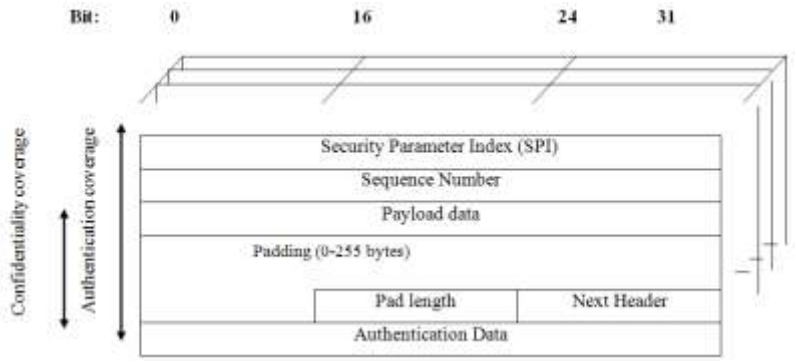


Figure 5: IPSec ESP Header

2.6 S/Mime (Secure/Multipurpose Internet Mail Extension)

S/MIME is the electronic standard that protects messages from unauthorized interception and forgery. S/MIME user public-key encryption technology to secure transmission, storage, authentication and forwarding of secret data, where SSL secures a connection between a client and a server over an insecure network, S/MIME is used to secure users, applications and computers. S/MIME is a security enhancement to the MIME (Multipurpose Internet Mail Extension) Internet e-mail format standard based on technology from RSA data security. To define MIME, we need first to have a general understanding of the underlying e-mail format that it uses, namely MIME. MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer protocol)**[1,4]**.

- SMTP cannot transmit executable file or other binary objects. A number of schemes are in use for converting binary files into a text form that can be used by SMTP mail systems.
- SMTP cannot transmit text data that includes national language characters because these are represented by 8-bit codes with values of 128 decimal or higher and SMTP is limited to 7-bit ASCII.
- SMTP servers may reject message over a certain size.
- SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problem.

MIME is intended to resolve these problems in a manner that is compatible with existing RFC822 implementation. The MIME specification includes the following elements.

1. Five new message header fields are defined, which may be included in an RFC 822 header. These fields provide information about the body of the message.

2. A number of content formats are defined, thus standardizing representations that support multimedia electronic mail.
3. Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alternation by the mail system.

In terms of general functionality, S/MIME is very similar to PGP. Both offer the ability to sign and/or encrypt messages. S/MIME provides the following functions.

Enveloped data: This consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.

Signed data: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base 64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.

Clear-signed data: As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base 64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.

Signed and enveloped data: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted. Some practical applications of S/MIME are.

- Electronic data exchange: Digital signatures on contracts
- Financial messaging: Store and transfer bank statements
- Content delivery: Electronic bill payment
- Health care: Secure patient records and health claims

Like SSL, IPSec and S/MIME is based on RSA algorithm for digital signature and digital envelopes as shown in Table 2**[1,2,5]**.

Table 2: Security Protocols Overview

Protocol	**Summary**
SSL (**Secure Socket Layer**)	Allows a "Secure Pipe" between any two application for transfer of data and mutual authentication
IPSec (**IP Security Protocol**)	Standard for Cryptographically-based authentication, integrity and confidentiality services at the IP datagram layer
S/MIME (**Secure MIME**)	Guarantees the secure communication, storage, authentication and forwarding of secret data at the application level

In virtually all distributed environments, electronic mail is the most heavily used network-based application. It is also the only distributed application that is widely used across all architectures and vendor platforms. Users expect to be able to and do, send mail to others who are connected directly or indirectly to the Internet, regardless of host operating system of communications suite.

With the explosively growing reliance or electronic mail for every conceivable purpose, there grows a demand for authentication and confidentiality services. Two schemes standout as approaches that are likely to enjoy widespread use in the next few years: pretty good privacy (PGP) and S/MIME.

III. ADDITIONAL NETWORK TYPE SECURITY PROTOCOLS

3.1 Wireless Security Protocols

Various wireless security protocols were developed to protect home wireless networks. These wireless security protocols include WEP, WPA and WPA2 each with their own strengths and weaknesses. In addition to preventing uninvited guests from connecting to your wireless network, wireless security protocols encrypt your private data as it is being transmitted over the airwaves. Wireless networks are inherently insecure. In the early days of wireless networking, manufacturers tried to make it as easy as possible for end users. The out-of-the-box configuration for most wireless networking equipment provided easy (but insecure) access to a wireless network. Although many of these issues have since been addressed, wireless networks are generally not as secure as wired networks. Wired networks, at their most basic level, send data between two points, A and B, which are connected by a network cable. Wireless networks, on the other hand, broadcast data in every direction to every device that happens to be listening, within a limited range. Following are descriptions of the WEP, WPA and WPA2 wireless security protocols**[6]**.

3.1.1 Wired Equivalent Privacy (Wep)

The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well known security flaws, is difficult to configure and is easily broken.

3.1.2 Wi-Fi Protected Access (Wpa)

Introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a pre shared key (PSK), commonly referred to as WPA Personal and the Temporal Key Integrity Protocol (TKIP) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates.

3.1.3 Wi-Fi Protected Access Version 2 (Wpa2)

Based on the 802.11i wireless security standard, which was finalized in 2004. The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is sufficient (and approved) for use by the U.S. government to encrypt information classified as top secret it's probably good enough to protect your secrets as well.

3.2 Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz from fixed and mobile devices and building personal area networks (PAN). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops and PDA. These networks are termed "ad hoc" because of their shifting network topologies. Bluetooth is defined as a layer protocol architecture consisting of core protocols, cable replacement protocols, telephony control protocols and adopted protocols. Mandatory protocols for all Bluetooth stacks are: LMP, L2CAP and SDP. In addition devices that communicate with Bluetooth almost universally can use these protocols, HCI and RFCOMM **[7]**.

3.2.1 LMP

The Link Management Protocol (LMP) is used for set-up and control of the radio link between two devices. Implemented on the controller.

3.2.2 L2CAP

The Logical Link Control and Adaptation Protocol (L2CAP) used to multiplex multiple logical connections between two devices using different higher level protocols. Provides segmentation and reassembly of on-air packets.

3.2.3 SDP

The Service Discovery Protocol (SDP) allows a device to discover services offered by other devices and their associated parameters. For example when you use a mobile phone with a Bluetooth headset the phone uses SDP to determine which Bluetooth profiles the headset can use (Headset Profile, Hands Free Profile, Advanced Audio Distribution Profile (A2DP)etc.) and the protocol multiplexer settings needed for the phone to connect to the headset using each of them. Each service is identified by a Universally Unique Identifier (UUID) with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128).

3.2.4 RFCOMM

Radio Frequency Communications (RFCOMM) is a cable replacement protocol used to generate a virtual serial data stream. RFCOMM provides for binary data transport and emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer, i.e. it is serial port emulation. RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth. Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM.

3.3 Bluetooth Vs Wi-Fi (IEEE 802.11)

Bluetooth and Wi-Fi (The brand name for products using IEEE 802.11 standards) have some similar applications: setting up networks, printing or transferring files. Wi-Fi is intended as a replacement for high speed cabling for general local area network access in work areas. This category of applications is sometimes called wireless local area networks (WLAN). Bluetooth was intended for portable equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any setting and also works for fixed location applications such as smart energy functionality in the home (thermostats, etc.). Wi-Fi and Bluetooth are to some extent complementary in their applications and usage. Wi-Fi is usually access point-centered, with an asymmetrical client-server connection with all traffic routed through the access point, while Bluetooth is usually symmetrical, between two Bluetooth devices. Bluetooth serves well in simple applications where two devices need to connect with minimal configuration like a button press, as in headsets and remote controls, while Wi-Fi suits better in applications where some degree of client configuration is possible and high speeds are required, especially for network access through an access node. However, Bluetooth access points do exist and ad-hoc connections are possible with Wi-Fi though not as simply as with Bluetooth**[8].** Wi-Fi Direct was recently developed to add a more Bluetooth like ad-hoc functionality to Wi-Fi.

3.4 Wireless Sensor Networks

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks (i) SNEP (ii) µTESLA. SNEP includes data confidentiality, two-party data authentication and evidence of data freshness. µTESLA provides authenticated broadcast for severely resource-constrained environments**[9]**.

A wireless sensor network (WSN), sometimes called a wireless sensor and actor network (WSAN) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure etc. 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. The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one or sometimes several sensors. Each such sensor network node has typically several parts i.e. a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network.

IV. CONCLUSSION

Protocols are sets of standards that define operations and how they will be done. Without protocols there would be much confusion and there would be no standard to allow computers to communicate. Protocols are a set of defined reactions to given events. When a traffic light turns red, the defined reaction should be to stop. This is a simple form of a protocol. Protocols are used for various purposes in the computer field. Protocols are mainly used to define networking standards. When dealing with networking then term network model and network layer used often. Network models define a set of network layers and how they interact. There are several different network models the most important two are: (1) TCP/IP Model - This model is sometimes called the DOD model since it was designed for the department of defense. It is also called the internet model because TCP/IP is the protocol used on the internet. (2) OSI Network Model - The International Standards Organization (ISO) has defined a standard called the Open Systems Interconnection (OSI) reference model. Currently there are many types of network available to establish communication between different types of devices. These networks uses different types of security protocols. While protocols can vary greatly in purpose and sophistication, most specify one or more of the following properties.

(i) Detection of the underlying physical connection (wired or wireless) or the existence of the other endpoint or node

(ii) Handshaking (dynamically setting parameters of a communications channel)

(iii) Negotiation of various connection characteristics

(iv) How to start and end a message

(v) How to format a message

(vi) What to do with corrupted or improperly formatted messages (error correction)

(vii) How to detect unexpected loss of the connection and what to do next

(viii) Termination of the session and or connection.

REFERENCES

[1]. Singh Brijendra., "Network Security and Management", Prentice Hall of India Private Limited, New Delhi-110001, Published in 2007.

[2]. Stalling, William. "Network Security Essentials application and standards", Third Edition, Pearson Prentice Hall, Published in 2008.

[3]. Silberschatz Abraham, Galvin Peter B., Gange Greg, "Operating System Concepts", 8th Edition, Wiley India Private Limited, New Delhi, Published in 2010.

[4]. Basandra Suresh Kumar," Computer Today", Galgotia publication Pvt. Ltd, New Delhi, Revised Edition 2008.

[5]. Stalling, William "Cryptography and Network Security", Fourth Edition, Pearson Prentice Hall, Published in 2006.

[6]. http://www.dummies.com/how-to/content/wireless-security-protocols-wep-wpa-and-wpa2.html; Retrieved on dated 18 March 2015.

[7]. http://en.wikipedia.org/wiki/Bluetooth; Retrieved on dated 07 April 2015.

[8]. http://en.wikibooks.org/wiki/Network_Plus_Certification/Technologies/Common_Protocols; Retrieved on dated 12 April 2015.

[9]. http://en.wikipedia.org/wiki/Wireless_sensor_network; Retrieved on dated 15 April 2015.