CHAPTER 3

COMMUNICATION SECURITY FRAMEWORK FOR REAL-TIME SYSTEM

3.1 INTRODUCTION

Human’s thirst to reach the hitherto unexplored frontier and recent advances in technology lead to situations which force us to prepare for several new challenges. As an example, stationing scientists in the space for a considerably long period for the purpose of research or soldiers in the front line of battlefield poses very peculiar, tough and sensitive challenges.

In these kind of situations, wherein scientists or soldiers need urgent medical attention at a reasonable cost at the quickest possible time, real-time systems come into help. It has been demonstrated successfully that surgeons are able to perform an operation on a patient 7000 km away with the help of robot and dedicated high-speed low latency communication infrastructure.

Governments all over the world are struggling with the task of providing quality health care to its citizens who are in remote hilly areas, scattered small hamlets at the need of the hour at the quickest possible time. Establishing sophisticated multi-specialty hospital with all specialists at these places are not cost effective and finding suitable experts are very difficult. Communication technology has matured well and is now available in almost all places with acceptable quality (Timothy Ramteke 2004). To become cost
effective so as to reach small and far away communities and hostile places, technology should allow the usage of secure and reliable shared networks which will provide acceptable latency with high security.

3.2 ISSUES AND CHALLENGES

One of the important issues in the spread of varies components of real-time system to multiple locations is connecting them together with communication link which guarantees high security, ensures strict adherence to the QOS parameters (Quing Li and Caroline Yao 2006) and incurs least cost.

A public network, like the public telephone system and the Internet, is a large collection of unrelated peers that exchange information more or less freely with each other (Chalie Kaufman et al 2002). The users with access to the public network may or may not have anything in common, and an user on that network may only communicate with a small fraction of potential users.

A private network is composed of computers owned by a single organization that share information specifically with each other. They are assured that they are going to be the only ones using the network, and that information sent between them will only be seen by members of the group. The typical corporate Local Area Network (LAN) or Wide Area Network (WAN) is an example of a private network. The line between a private and public network has always been drawn at the gateway router, where an organization will erect a firewall to keep intruders from the public network out of their private network, or to keep their own internal users from perusing the public network.
As collaboration between different entities located at different places of an organization increases, it becomes necessary to interconnect different networks situated in various locations together. This was traditionally done using leased phone lines of varying speeds. By using leased lines, an organization can be assured that the connection is always available and private. Leased phone lines, however, can be expensive. They are typically billed a flat monthly fee, plus mileage expenses. Private networks also have trouble handling roving users. If a roving user is not near the organization computers, the user has to dial organization's modem located faraway, which is an extremely expensive proposition.

In many cases, long-haul connections of networks are done with a leased line, a connection to a frame relay network, or ISDN. Frame relay lines can also give high speeds without the mileage charges. Purchasing a connection to a frame cloud will connect the peers through switches. Unlike a leased line, the amount payable is based more on the bandwidth that is committed to the circuit than distance. Frame connections are still somewhat expensive, however. ISDN, like the plain old telephone system, incurs long-distance charges. In many locations, the local telephone company charges per minute even for local calls, which again runs expenses up. For situations where corporate office networks are in separate cities, having each office get a T1, frame relay, or ISDN line to an ISP’s local POP would be much cheaper than connecting the two offices using these technologies.

The design of the proposed communication security framework for real-time system to spread the real-time application to all places takes care of the above mentioned issues.

- Secures private network from public network by firewall and IDS
• Minimizes the recurring expenditure incurred for connecting different network of collaborating entities

• Ensures required QOS parameters for the real-time communication by ensuring enhanced performance of individual components

• Ensures private communication over a public medium

The objective of the proposed communication security framework for real-time system is to create a secure, private network over a public network. This is achieved by Virtual Private Network (VPN). This can be created using software, hardware, or a combination of the two that creates a secure link between peers over a public network. This is done through encryption, authentication, packet tunneling, and firewalls. Because they skirt leased line costs by using the Internet as a WAN, VPNs are more cost-effective.

A virtual private network is a way to simulate a private network over a public network, such as the Internet. It is called "virtual" because it depends on the use of virtual connections—that is, temporary connections that have no real physical presence, but consist of packets routed over various machines on the Internet on an ad hoc basis. Secure virtual connections are created between two machines, a machine and a network, or two networks.

Using the Internet for remote access saves a lot of money. User will be able to dial in wherever Internet Service Provider (ISP) has a Point-Of-Presence (POP). If an ISP with nationwide POPs is chosen, there's a good chance that LAN will be a local phone call away. Some ISPs have expanded internationally as well, or have alliances with ISPs overseas. Even many of the smaller ISPs have toll-free numbers for their roaming users. At any rate,
well-chosen ISP accounts should be cheaper than setting up a modem pool for remote users and paying the long-distance bill for roaming users. Even toll-free access from an ISP is typically cheaper than having own toll-free number.

A VPN could then be instituted between the routers at the two places, over the Internet. In addition, a VPN will allow to consolidate Internet and WAN connections into a single router and single line, saving money on equipment and telecommunications infrastructure.

### 3.3 REAL-TIME SYSTEM

It is common to come across several real-time applications in everyday life like digital control, optimal control, command and control, signal processing, tracking, real-time databases, multimedia and tele-surgery. To gauge the relative characteristics of these applications, abstract workload model could be a good starting point. As a simplest representative real-time system, digital controller is explained below (Jane 2007).

Many real-time systems are embedded in sensors and actuators and function as digital controllers. The term plant in the block diagram Figure 3.1 refers to a controlled system, for example, an engine, a break, an aircraft, a patient. The state of the plant is monitored by sensors and can be changed by actuators. The real-time computing system estimates from the sensor readings the current state of the plant and computes a control output based on the difference between the current state and the desired state (called reference input in the Figure 3.1). This computation is called the control-law computation of the controller. The output thus generated activates the actuators, which bring the plant close to the desired state.
As an example, an analog single-input or single-output PID (Proportional, Integral, and Derivative) controller is explained. The analog sensor reading $y(t)$ gives the measured state of the plant at time $t$. Let $e(t) = r(t) - y(t)$ denote the difference between the desired state $r(t)$ and the measured state $y(t)$ at time $t$. The output $u(t)$ of the controller consists of three terms: a term that is proportional to $e(t)$, a term that is proportional to the integral of $e(t)$ and a term that is proportional to the derivative of $e(t)$.

In the sampled data version, the input to the control-law computation are the sampled values $y_k$ and $r_k$, for $k = 0, 1, 2, ..., $ which analog-to-digital converters produce by sampling and digitizing $y(t)$ and $r(t)$ periodically every $T$ units of time. $e_k = r_k - y_k$ is the $k^{th}$ sample value of $e(t)$.

$$u_k = u_{k-2} + \alpha e_k + \beta e_{k-1} + \gamma e_{k-2}$$

(3.1)

where $\alpha$, $\beta$ and $\gamma$ are proportional constants. During the $k^{th}$ sampling period, the real-time system computes the output of the controller according to this expression. From the above equation (3.1), it can be see that during any sampling period (say the $k^{th}$), the control output $u_k$ depends on the current and past measured values $y_i$ for $i \leq k$. The future measured values $y_i$’s for $i > k$ in turn depend on $u_k$. Such a system is called a feedback control loop or simply a loop.
It can be implemented as an infinite timed loop:

set timer to interrupt periodically with period \( T \);
at each timer interrupt,
do
do analog-to-digital conversion to get \( y \);
compute control output \( u \);
output \( u \) and do digital-to-analog conversion;
end do;

![Digital Controller Diagram](image)

**Figure 3.1 A digital controller**

### 3.4 SELECTION OF SAMPLING PERIOD

The length \( T \) of time between any two consecutive instants at which \( y(t) \) and \( r(t) \) are sampled is called the sampling period. The behaviour of the resultant digital controller critically depends on this parameter. To arrive at an optimal sampling period \( T \), two factors needed to be considered. The first is the perceived responsiveness of the overall system (i.e., the plant and the controller). Often, the system is operated by a person (example, a driver). The operator may issue a command at any time, say at \( t \). The consequent change in the reference input is read and reached to by the digital controller at the next sampling instant. This instant can be as late as \( t + T \). Thus, sampling
introduces a delay in the system response. The operator will feel the system sluggish when the delay exceeds a tenth of a second. Therefore, the sampling period of any manual input should be under this limit.

The second factor is the dynamic behaviour of the plant. It is desirable to keep the oscillation in its response small and the system under control. To illustrate, the disk drive controller can be considered. The plant in this example is the arm of a disk (Astrom and Wittenmark 1997). The controller is designed to move the arm to the selected track each time when the reference input changes. At each change, the reference input $r(t)$ is a step function from the initial position to the final position. In Figure 3.2 these positions are represented by 0 and 1, respectively, and the time origin is the instant when the step in $r(t)$ occur. The dashed lines in Figure 3.2 give the output $u(t)$ of the analog controller and the observed position $y(t)$ of the arm as a function of time. The solid lines in the lower and upper graphs gives, respectively, the analog control signal constructed from the digital outputs of the controller and the resultant observed position $y(t)$ of the arm. At the sampling rate shown here, the analog and digital versions are essentially the same. The solid lines in Figure 3.3 gives the behaviour of the digital version when the sampling period is increased by 2.5 times. The oscillatory motion of the arm is more pronounced but remains small enough to be acceptable. However, when the sampling period is increased by five times, as shown in Figure 3.4, the arm requires larger control to stay in the desired position: When this occurs, the system is said to have become unstable. In general, the faster a plant respond to changes in the reference input, the faster the input to its actuator varies, and the shorter the sampling period.
Figure 3.2 Effect of sampling period

Figure 3.3 Effect of sampling period with 2.5 times increased sampling period
Figure 3.4 Effect of sampling period with 5 times increased sampling period

3.5 COMMUNICATION SECURITY FRAMEWORK FOR REAL-TIME SYSTEM

Complex Real-Time applications like remote surgery system moves the real-time computing system which computes control output from the plant, sensors and actuators to far away distance of order of thousands of kilometers. Challenges here by moving it to farther place are the delay in communication, availability and security. This work aims at designing a frame work for such real-time systems. Figure 3.5 illustrates a typical real time system with proposed communication security frame work.

Main aim of this research is to speed up the operation without sacrificing accuracy of the total system. For this task, soft computing techniques DT and RIPPER which provide for excellent opportunity to parallelize the prediction operation of IDS and thereby allowing the overall performance improvement in the resultant communication system supporting real-time system are selected. The particular case, which the study has been
selected for the purpose of arriving at system requirement parameters and to rank the perceived threat to such real-time system, is telesurgery.

![Proposed communication security framework for real-time system](image)

**Figure 3.5** Proposed communication security framework for real-time system

This kind of systems are particularly very sensitive to delay, delay variations and bandwidth variations (Krishna and Shin 1997). These parameters must be guaranteed for their correct and smooth functioning. At the same time the proposed strategy must satisfy these requirements with a least cost.

So, the ultimate choice leads to the use of shared data network, which will guarantee the necessary bandwidth. Since, these real-time systems are very sensitive and cannot be suspended at the middle, all systems must provide the desired service throughout the procedure. So, the system is proposed in which at least two layers of communication options are kept ready. One is a shared network that will primarily be used and other one is dial-up stand by network.
The model proposes an encrypted tunnel from the router to which control-law computing system connects to the other router, which directly connects to the sensors, actuators and plant. All communications between these two routers must be encrypted which will ensure both privacy, and integrity. Since, small deviation of the real-time system from its expected performance may be fatal to the system, integrity of the message transferred between the two ends must be protected.

Major threats are from the Denial of Service (DOS) and Distributed Denial Of Service (DDOS) attacks which will eventually limit the available bandwidth between two ends. This must be continuously monitored and responded quickly. For this, the study has constructed and analyzed intrusion detection models based on the RIPPER and DT. Performance of the constructed IDS models are improved by parallel implementation.

3.6 FIREWALL

A firewall is a system or group of systems that enforces an access control policy between two networks. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. A firewall enables you to permit traffic that you want and keep out the things you don’t.

3.6.1 Types of Firewalls

Firewalls are available in three different types as explained in detail below based on the information they rely on for their decision and their ability to remember the past events.
3.6.1 Packet filters

In its most basic form, a packet filter makes decisions about whether to forward a packet based only on information found at the IP or Transmission Control Protocol (TCP)/User Datagram Packet (UDP) layers; in effect, a packet filter is a router with some intelligence. However, a packet filter only handles individual packets; it does not keep track of TCP sessions. Thus, it is poorly equipped to detect spoofed packets that come in through an outside interface, pretending to be part of an existing session by setting the Acknowledge (ACK) flag in the TCP header. Packet filters are configured to allow or block traffic according to source and destination IP addresses, source and destination ports, and type of protocol (TCP, UDP, Internet Control Message Protocol [ICMP], and so on).

Packet filter does not have to do any inspection of application data. It can operate nearly as fast as a router that is performing only packet routing and forwarding. But, it has inability to detect spoofing. The packet filter concept has been improved trying to overcome this handicap.

3.6.1.2 Stateful inspection packet filters

The concept of stateful inspection came about in an effort to improve on the capability and security of regular packet filters while still capitalizing on their inherent speed. A packet filter with stateful inspection is able to keep track of network sessions, so when it receives an Acknowledgement (ACK) packet, it can determine its legitimacy by matching the packet to the corresponding entry in the connection table. An entry is created in the connection table when the firewall sees the first Synchronize (SYN) packet that begins the TCP session. This entry is then referred for
succeeding packets in the session. Entries are automatically timed out after some configurable timeout period.

Stateful inspection packet filters remain speed kings of firewalls and are most flexible where new protocols are concerned, but they are sometimes less secure than application proxies.

3.6.1.3 Application proxies

![Application proxy data flow](image)

**Figure 3.6 Application proxy data flow**

As the name implies, application proxy firewalls act as intermediaries in network sessions. The user’s connection terminates at the proxy, and a corresponding separate connection is initiated from the proxy to the destination host. Connections are analyzed all the way up to the application layer to determine if they are allowed. It is this character that gives proxies a higher level of security than packet filters, stateful or not. However, this additional processing extracts a toll on performance. Figure 3.6 shows how packet processing is handled at the application layer before it is passed on or blocked. One potentially significant limitation of application proxies is that as new application protocols are implemented, corresponding proxies must be developed to handle them.
3.7 VPN CONCEPT

The important concepts that VPN uses to protect data travelling across the Internet are authentication, encryption, and tunneling (Charlie Scott et al 1999).

3.7.1 Authentication

Authentication techniques are essential to VPNs, as they ensure the communicating parties that they are exchanging data with the correct user or host. Authentication is analogous to "logging in" to a system with a username and password. VPNs, however, require more stringent authentication methods to validate identities. Most VPN authentication systems are based on a shared key system. The keys are run through a hashing algorithm, which generates a hash value. The other party holding the keys will generate its own hash value and compare it to the one it received from the other end. The hash value sent across the Internet is meaningless to an observer, so someone sniffing the network wouldn't be able to glean a password.

Authentication can also be used to ensure data integrity. The data itself can be sent through a hashing algorithm to derive a value that is included as a checksum on the message. Any deviation in the checksum sent from one peer to the next means the data was corrupted during transmission, or intercepted and modified along the way.

3.7.2 Encryption

Security and data confidentiality are prime requirements for any VPN. These are provided by encrypting the data before transmitting through the public network and decrypted before being used.
3.7.3 Tunneling

A key component of the VPN is tunneling, a vehicle for encapsulating packets inside a protocol that is understood at the entry and exit points of a given network. These entry and exit points are defined as tunnel interfaces.

<table>
<thead>
<tr>
<th>IP</th>
<th>IPsec</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier Protocol</td>
<td>Encapsulating Protocol</td>
<td>Passenger Protocol</td>
</tr>
</tbody>
</table>

**Figure 3.7 Tunneling packet format**

Tunneling involves three types of protocols as shown in Figure 3.7. Firstly the passenger protocol which is the protocol being encapsulated. Secondly, the encapsulating protocol which is used to create, maintain and tear down the tunnel. Thirdly, the carrier protocol which is used to carry the encapsulated packet. IP is the popular carrier protocol because of its robust routing capabilities, ubiquitous support across different media and deployment within the Internet.

3.8 INTERNET PROTOCOL SECURITY

Internet Protocol Security (IPSec) is a suite of network-layer protocols that extends IP by providing mechanisms for authentication, confidentiality, and integrity in IP communications. With the use of IPSec, a communication session between two hosts can be encrypted in a way that is transparent to applications running on the hosts.
3.8.1 Implementation

IPSec has two security protocols that can be implemented separately or together:

- Authentication Header (AH): Performs authentication of sender only. Authentication can be performed using Message Digest 5 (MD5), hash-based message authentication code (HMAC), or Secure Hash Algorithm-1 (SHA-1).

- Encapsulating Security Protocol (ESP): Performs both authentication of sender and encryption of data. Authentication can be performed using the algorithms described previously, while encryption can be performed using Digital Encryption Standard (DES), Triple DES (3DES), Blowfish, International Data Encryption Algorithm (IDEA), Cast, RC5, and other algorithms (William Stallings 2003).

At the center of VPN is the encrypted tunnel (or VPN link) created using the IKE/IPSec protocols. The peers negotiating a link first create a trust between them. This trust is established using certificate authorities, PKI or pre-shared secrets. Methods are exchanged and keys created. The encrypted tunnel is established and then maintained for multiple connections, exchanging key material to refresh the keys when needed. A single gateway maintains multiple tunnels simultaneously with its VPN peers. Traffic in each tunnel is encrypted and authenticated between the VPN peers, ensuring integrity and privacy. Data is transferred in bulk via these virtual-physical links.
3.9  INTERNET KEY EXCHANGE

In symmetric cryptographic systems, both communicating parties use the same key for encryption and decryption. The material used to build these keys must be exchanged in a secure fashion. Information can be securely exchanged only if the key belongs exclusively to the communicating parties.

The goal of the Internet Key Exchange (IKE) is for both sides to independently produce the same symmetrical key. This key then encrypts and decrypts the regular IP packets used in the bulk transfer of data between VPN-1 Power peers. IKE builds the VPN tunnel by authenticating both sides and reaching an agreement on methods of encryption and integrity. The outcome of an IKE negotiation is a Security Association (SA). This agreement upon keys and methods of encryption must also be performed securely. For this reason IKE is composed of two phases. The first phase lays the foundations for the second.

Diffie-Hellman (DH) is that part of the IKE protocol used for exchanging the material from which the symmetrical keys are built. The Diffie-Hellman algorithm builds an encryption key known as a “shared secret” from the private key of one party and the public key of the other. Since the IPSec symmetrical keys are derived from this DH key shared between the peers, at no point are symmetric keys actually exchanged.

3.10  PUBLIC KEY INFRASTRUCTURE (PKI)

X.509-based PKI solutions provide the infrastructure that enables entities to establish trust relationships between each other based on their mutual trust of the Certificate Authority (CA). The trusted CA issues a
certificate for an entity, which includes the entity’s public key. Peer entities that trust the CA can trust the certificate — because they can verify the CA’s signature — and rely on the information in the certificate, the most important of which is the association of the entity with the public key.

A VPN peer taking part in a VPN tunnel establishment must have an RSA key pair and a certificate issued by a trusted CA. The certificate contains details about the module’s identity, its public key, Certificate Revocation List (CRL) retrieval details, and is signed by the CA.

When two entities try to establish a VPN tunnel, each side supplies its peer with random information signed by its private key and with the certificate that contains the public key. The certificate enables the establishment of a trust relationship between the gateways; each gateway uses the peer gateway’s public key to verify the source of the signed information and the CA’s public key to validate the certificate’s authenticity. In other words, the validated certificate is used to authenticate the peer.

3.11 THE NEED FOR VIRTUAL PRIVATE NETWORKS

Communicating parties need a connectivity platform that is not only fast, scalable, and resilient but also provides confidentiality, integrity, and authentication.

Confidentiality

Only the communicating systems must be able to read the private information exchanged between them.
Authentication

The communicating systems must be sure that they are connecting to the intended party.

Integrity

The sensitive data passed between the communicating systems is unchanged, and this can be proved with an integrity check.

3.12 VPN WORKING PROCESS

![Diagram](image)

**Figure 3.8 Confidentiality, integrity and authentication via IPSec**

In Figure 3.8, host 1 and host 6 need to communicate. The connection passes in the clear between host 1 and the local gateway. From the source and destination addresses of the packet, the gateway determines that this should be an encrypted connection. If this is the first time the connection is made, the local gateway initiates an IKE negotiation with the peer gateway in front of host 6. During the negotiation, both gateways authenticate each other, and agree on encryption methods and keys. After a successful IKE negotiation, a VPN tunnel is created. From now on, every packet that passes between the gateways is encrypted according to the IPSec protocol. IKE supplies authenticity that is gateways are sure they are communicating with each other and creates the foundation for IPSec. Once the tunnel is created,
IPSec provides privacy through encryption and integrity via one-way hash functions.

After a VPN tunnel has been established (Figure 3.8), packets are dealt with in the following way:

- A packet leaves the source host and reaches the gateway.
- The gateway encrypts the packet.
- The packet goes down the VPN tunnel to the second gateway. Actually the packets are standard IP packets passing through the Internet. However, because the packets are encrypted, they can be considered as passing through a private “virtual” tunnel.
- The second gateway decrypts the packet.
- The decrypted packet is delivered to the destination host. From the perspective of hosts, they are connecting directly.

3.13 IDS

Intrusion detection an important component of information security technology helps in discovering, determining, and identifying unauthorized use, duplication, alteration, and destruction of information and information systems. Intrusion detection relies on the assumption that information and information systems under attack exhibit several distinguishable behavioral patterns or characteristics to that of the normal ones.
3.14 SUMMARY

The communication security framework for real-time system plays an important role in mitigating the security risk of exposing the sensitive real-time system to the ever increasing novel attacks emanating from the public network. The communication security framework for real-time system is presented with all its components. The proposed framework considers multiple classes of real-time systems with different QOS requirements. Three important components of the proposed system are Firewall, VPN and IDS.

The introspection of the frame work makes clear that it ensures secure private communication over insecure public media without sacrificing any QOS parameters with minimum expenditure.