Chapter 5 Performance parameters for the proposed protocol

In the previous chapter the authors reviewed various systems where a trust based relationship is required by two previously unknown computers in order to exchange sensitive data between them. The authors concluded that an e-commerce system with an online payment option is most suitable system to assess strengths and weaknesses of their protocol against other standard protocols. The authors also presented generic architecture of an e-commerce system for online payment and showed that their protocol is focused on strengthening communication between the client and the server with help of a trusted third party.

This chapter begins with discussion on why simulation is required for the protocol. The authors also discuss the need for simulation for testing performance of the proposed protocol compared to other industry standard protocols.

5.1 Need for Simulation

Simulation is an attempt to model real life hypothetical situations on a computer so that it can be studied to see how the system works.

A simulation is used when it is not possible to experiment in real life. The protocol presented in this thesis is also difficult to implement in real life. Simulation for testing the protocol is required due to following reasons:

1) Simulation is done in order to test the protocol in an E-Commerce system virtually to find out its areas of strengths and weaknesses.
2) Simulation is conducted to compare the protocol with other industry standard protocols such as IKP, 3D Secure and other significant protocols discussed later in this chapter.
3) Simulation is carried out to compare the number of operations required by authors’ protocol against other industry standard protocols. This will help in deciding which protocol is faster.
4) A simulation of the protocol is done in order to find out battery usage of authors’ protocol against industry standard protocols and to discern the battery efficient protocol.
5) A simulation will give a considerable insight into performance of the proposed protocol against industry standard protocols on different wireless network bandwidth.
5.2 Industry Standard Protocols and other Key Exchange Protocols used for Comparison in Simulation

A composition of industry standard protocols and modern key exchange protocols were used in simulation to compare their performance with the proposed protocol. Following protocols were used in simulation.

1) SET [106]
2) IKP [107]
3) 3D Secure [108]
4) Lee, Chan & Chan’s Protocol [109]
5) Xie, Qi et al.’s Protocol [110]
6) Kungpisdan, Srinivasan & Dung Le’s Protocol [97]
7) Issac & Camara’s Protocol [111]
8) Sekhar & Sarvabhatla’s Protocol [96]

Secure Electronic Transaction is a standard of communication protocol that is used to perform secure transaction over insecure networks such as Internet. This protocol is used in mostly credit/debit card applications. SET was one of the first protocols to provide secure transactions using credit cards on Internet. SET was selected for simulation as it was one of the major standard protocols used in industry before it was discontinued. SET used a double signature system. A double signature system was developed to separate information of customer’s order from bank and payment details from merchant. This way it provided double protection to customer. [106]

Internet Keyed Payment protocol is developed by IBM research labs to address issues which most protocols failed to address at the beginning of E-Commerce on Internet. The IKP protocol is an open source protocol, browser, server and hardware independent. The IKP protocol is designed to work with not only credit cards but other payment systems as well. This protocol can be extended from two party to multi party key exchange protocol which makes it an suitable candidate for testing against the protocol proposed in this thesis. [107]

3D Secure protocol is proposed by Visa and MasterCard. It is a XML based protocol that provides additional layer of security to online transaction over insecure networks. This protocol adds an extra step of authentication via OTP before payment making the transaction more secure.
Being one of the leading protocols in the field makes this protocol an interesting choice for simulation. [108]

Lee, Chan & Chan’s protocol is an extension of proposed three party protocols with some vulnerabilities. This protocol is claimed to be one of the most superior three party encrypted key exchange protocols according to authors [109]. This protocol was selected for simulation due to superiority factor claimed its creators.

Xie, Qi et al. in their paper propose a three party password based authentication key exchange protocol. The protocol is developed for resource constrained mobile based devices that lets them communicate securely over an insecure network [110]. As the protocol is specifically developed for resource constrained mobile based devices it makes it ideal for simulation and comparison against protocol proposed in this thesis.

Kungpisdan et al.’s protocol is a mobile based payment protocol which according to authors is also suitable for wireless networks [97]. This protocol uses concepts of symmetric key cryptography and has lower computation requirements as claimed by authors. This protocol also satisfies requirements of transaction security set in place by protocols such as SET and IKP. A unique point about this protocol is that the credit card information is not required to be sent during transaction that makes the system more secure. It is due to protocol’s design that it is suitable for wireless networks and has lower computational requirements and compliance with transaction security properties that made this protocol part of simulation.

Issac & Camara’s protocol assumes that full connectivity is not always possible between the entities involved in transaction. The authors propose an anonymous protocol with digital signatures and message recovery using public keys that makes it possible to perform transaction even when full connectivity is not available. It is due to this unique property that this protocol has been selected for simulation. [7]

In their paper Sekhar & Sarvabhatla present a secure mobile payment protocol. According to authors this protocol is suitable for wireless network and is based on symmetric key cryptography [96]. They compare their protocol with SET and IKP protocols based on number of operations and claim that their protocol satisfies more security requirements than SET and IKP.
protocols. It is due to this claim by its authors that this protocol is included in the list of protocols for simulation in this thesis.

5.3 Simulation Criteria

Simulation criteria in this thesis are selected based on characteristics of protocol and similar simulations carried out by other researchers [96] during their work on key exchange protocols. To understand the selection of criteria for the simulation, it is important to understand requirements for the protocol. The protocol is expected to primarily work on mobile devices. Mobile devices communicate with one or the other wireless communication system. Therefore, the protocol must be able to communicate using wireless medium. The protocol is designed to be operational on mobile devices. It is assumed that these mobile devices have limited processing power. Therefore, they are not suitable for complex computations required for key generation.

The protocol is expected to be simple and least resource intensive on clients with limited resources. All mobile devices have limited battery power. If the protocol performs complex operations on client's side, it will require more battery power. The protocol should also be using least amount of battery power to do most part of work.

In a country like India, where there are areas in which connectivity is limited, the internet bandwidth is very low. The protocol should be able to perform key exchange function even on lower bandwidth. Therefore, performance of protocol on different bandwidths is also a criterion.

There are different devices with different configurations. The protocol should be able to function on all kinds of wireless devices and give optimum performance. Therefore, different type of devices becomes a criterion as well. Therefore, following criteria were chosen to evaluate the proposed protocol in this thesis: 1) number of operations; 2) battery backup; 3) Internet bandwidth and 4) suitability for wireless devices.

5.3.1 Number of Operations

According to Sarvabhatla [96] the number of operations of the protocol specifies how many operations the processor has to undertake in order to send the key to the recipient from a trusted third party. This criterion highlights the time factor of the protocol. The higher the number of operations, the more time it will take for the protocol to exchange the key. This criterion is also directly proportional to speed of processor. Higher
processor speed means less time it will take to perform the operation. In this thesis the number of operations from a trusted third party is considered.

5.3.2 Battery Backup
According to Hongyang [112] and Guo and Ma [113], battery usage is a critical factor for any mobile based software or hardware. The protocol in this thesis is designed for wireless devices. All wireless devices run on limited battery backup. This makes it imperative that the protocol should be battery friendly. Optimization of protocol leads to battery friendliness of protocol. Another factor that affects battery usage of protocol is computational complexity. If the protocol has complex operations that are computationally intensive that may affect battery usage.

5.3.3 Internet Bandwidth
According to Carl et al. [114], bandwidth plays a crucial role in performance of key exchange protocols that use timestamps. Internet speed in India is one factor that is needed to be considered when testing the protocol in this thesis. The performance of many applications in wireless devices depends on Internet bandwidth that is accessible from device. There are applications that do not operate properly on low bandwidth. Another issue is how different bandwidths or mediums to access the data affect battery usage. According to an online article [115], 2g data network has a high battery drain, 3g data network uses twice as much battery as 2g if the signal is not strong, Wi-Fi signal is continuous and does not drain as much power as the other two. Hence, the bandwidth is an important parameter to consider when testing a protocol.

5.3.4 Wireless Devices
As discussed in chapter 4, the mobile revolution has brought a large number of companies manufacturing various different models with variety of configurations. There are devices with wide configurations of processors, memory, display and battery backup. Due to this variation on device configuration it is important that the protocol is tested on different parameters to ascertain its performance on above mentioned criteria.

5.4 Simulation and Deployment Details
For the purpose of this simulation a sample e-commerce mobile application was developed and was installed in phones and tablets configurations of which are discussed in previous chapter. A
server application for e-commerce system was also developed that was installed in laptop with web server. A PHP web service was also developed. The role of this server is to provide service of key generation and distribution.

Following assumptions are made for simulation:

1) Both the client and server have their own private keys.  
2) Both client and server have shared their private key with a trusted third party.  
3) The client and server are in an unaltered form and are not compromised in any way by a malicious user.  
4) The third party is unaltered and not compromised in any way by a malicious user.  
5) A malicious user has the ability to intercept the packets travelling on network and analyze their contents.

A single execution of the protocols returns results that are insignificant to measure the performance of the protocols. Hence, the protocols were executed in a cycle for a thousand times and the results were derived after completing this cycle for each of the protocols.

5.4.1 Logical Setup

The figure 5.1 portrays the general system architecture and flow of information step by step. There are three main components in this system: 1) mobile app (Alice); 2) web service (Bob) and 3) trusted third party.

**Fig. 5.1 Architecture**
The mobile app/Alice is the initiator of secure communication session. To begin the communication mobile application/Alice will send its ID and ID of web server/Bob to a trusted third party requesting the shared secret key.

The trusted third party will generate the key and integrate it with ticket and encrypt this with web server (Bob)’s secret key. It will also include synchronization sequence and the shared secret key for mobile application/Alice. This whole message will be encrypted in Alice’s private key and sent to Alice.

The trusted third party will also send synchronization sequence and ID of Alice to Bob encrypted by Bob’s secret key. This is done in order to verify Alice and synchronize Bob’s clock with synchronization sequence in order to detect a stale message.

Lastly, Alice receives the message from a trusted third party and decrypts the message and synchronizes the key. It then forwards the ticket to Bob with the shared secret key.

The future communication is encrypted by the shared secret key between Alice and Bob.

5.4.2 Implementation Details

Figure 5.2 illustrates the deployment of different components and various function calls with their arguments that takes place during key exchange process.

The authors are using an Android based mobile application for initiating communication. The mobile application sends its ID and ID of the computer it wants to communicate securely with to a trusted third party with help of Get_Key() function.

The trusted third party is implemented as a PHP based web service. The authors are not using any particular features of PHP scripting language, hence, other server side scripting languages providing web service feature can also be used for a trusted third party. The role of a trusted third party is to generate shared secret key using Generate_Key() function that returns a shared secret key in string format. The trusted third party generates a message for Bob with ID of Alice, shared secret key and time stamp. These contents of message are encrypted with Bob’s private key so that no one but Bob can decrypt the message. This whole message is then incorporated in a bigger message intended to Alice with the shared secret key, time stamp and synchronization sequence. This message is encrypted by Alice’s private key. The trusted third party also sends a synchronization sequence and ID of Alice to Bob through a separate message to synchronize Bob’s clock with help of synchronization.
sequence and as an indication for future communication from Alice. This message is also encrypted by Bob’s private key. This message is sent using SetSync() function. Bob is the recipient here for all communication from Alice and a trusted third party. Once the message from a trusted third party is received, Bob decrypts message and gets ID of Alice using Get_ID_Alice() function and set_Sync() function. Once Bob receives the message from Alice, it decrypts the message and gets shared secret key using Get_K_AB() function, time stamp using Get_Timestamps() function and ID of Alice using Get_ID_Alice() function.

**Fig. 5.2 Deployment Diagram**

The classes used for implementation are mentioned in fig. 5.3. Following description is of different classes, members and member functions that different components are using for key exchange process.

Alice: Alice is the communication initiator in this setup. Alice wishes to exchange information with Bob securely. In this set up Alice initiates communication with a trusted third party in order to get shared secret key with ticket which it will share with Bob. Alice is represented by a mobile application. Here, Alice is represented by DS_Alice class.

Bob: Bob is the receiver of communication. Bob receives the shared secret key from Alice along with a ticket from a trusted third party. The ticket from trusted third party helps Bob in bridging trust gap with previously unknown entity Alice. Bob also receives synchronization
sequence from a trusted third party to synchronize its clock with Alice in order to detect stale packets. Bob is represented by class DS_Bob.

Both DS_Alice and DS_Bob are developed with required members and member functions to perform necessary operations on class members.

Trusted Third Party: The trusted third party bridges gap of trust between Alice and Bob as these two are unknown to each other. The trusted third party has private keys of both Bob and Alice. Bob trusts message from Alice if it is accompanied by a ticket from a trusted third party. In this experiment the trusted third party is a PHP web service. The trusted third party also provides synchronization sequence to both Bob and Alice to synchronize their clocks in order to detect stale packets.

ID of sender and receiver: These IDs are used to identify sender and receiver. These are represented as members of class DS_Alice and DS_Bob.

Timestamp: Timestamp is a string mentioning current date and time. It is used for thwarting against replay type of attacks and checking freshness of message. Timestamp is represented as a member of class DS_Alice and DS_Bob.

Sync: Synchronization sequence generated by a trusted third party and is sent to both Alice and Bob in order to synchronize their clocks for thwarting replay type of attacks through resending of old messages. Synchronization sequence is represented as a member of classes DS_Alice and DS_Bob.

Shared Secret Key: The shared secret key is generated by a trusted third party and used by both Alice and Bob for sharing critical information. Shared Secret Key is represented as a member of class DS_Alice.
Fig. 5.3 Class Diagram