SUPERVISOR CERTICATE

IT IS CERTIFIED THAT THE FINAL COPY OF THESIS HAS BEEN EVALUATED BY ME, FOUND AS PER SPECIFIED FORMAT AND ERROR FREE.

_____

DR. IMRAN RASHID

ICMETRIC BASED SECURE COMMUNICATION

By

Shahzaib Tahir

A thesis submitted to the faculty of Information Security Department Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

APRIL 2015

ABSTRACT

Secure communication refers to successful and secure interaction among the participants having common intentions in one-to-one or group settings. One-to-one is termed as a decentralized communication environment where any party can initiate the communication. Whereas group is a dynamic environment composed of activities exhibited by individuals in a group where the number of participants are variable. Therefore the level of security in this environment needs to be given utmost importance. Both of the environments require maintaining secrecy of cryptographic keys which is often overlooked. ICMetric is an emerging technology that has gained importance because of its security advantages for embedded system applications. This technology resolves issues of key theft and storage, through the development of device fingerprint that can be used for secure key generation. This research discusses ICMetric in detail by elaborating its salient features. Authors enumerate the current research being carried out on ICMetric technology along with its areas of application. This research elucidates the changes that ICMetric technology has brought to conventional cryptosystem design.

This research proposes two state of the art symmetric cryptographic frameworks for the one-to-one and group communication. Both of the frameworks are based on the utilization of the ICMetric technology. Furthermore this research sheds light on the advantages of utilizing the proposed frameworks in a resource constrained environments by performing an in depth security analysis and performance evaluation of the frameworks.

DEDICATION

“In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my parents, sister, brother and my teachers.

ACKNOWLEDGEMENT

My utmost debt of gratitude is to my supervisor Dr. Imran Rashid. It has been an honor to study under his supervision. I appreciate all his generous contributions of time, ideas, and guidance to make my final year project both productive and stimulating. I am also thankful for the excellent example he has provided as a successful researcher.

I would also like to thank my committee member and HOD Dr. Baber Aslam for his constant support during this project and my studies. His guidance during the course work encouraged me to actively get involved in research and development. I would also like to thank my other committee members Mr. Waleed Bin Shahid and Mr. Muzammil Ahmed Khan for their time, interest, and helpful comments.

I am highly thankful to all my teachers who have been guiding me throughout my course work and have helped increase my knowledge. I am also thankful to Dr. Mehreen Afzal for her constant guidance and training related to cryptography that enabled me to carry out this research and development work.

Lastly, I would like to thank my family for all their love and encouragement. For my parents who raised me with a love of science and supported me in all my pursuits. And most of all for my loving, supportive and encouraging sister and brother whose faithful support during the final stages of my degree is so appreciated. Thank you it would not have been possible without you.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

KEY TO ACRONYMS

ICM	ICMetric
GC	Group Controller
KDM	Key Distribution Manager
AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
XOR	Exclusive OR
SHA	Secure Hash Algorithm
I/O	Input/Output
OFT	One-Way Function Key Tree
DoS	Denial of Service
DDos	Distributed Denial of Service
IoT	Internet of Things
CIA	Confidentiality, Integrity, Availability
SOCP	Secure One-to-One Communication Protocol
EGCP	Euclidean based Group Communication Protocol
SRP	Secure Remote Password Protocol
IT	Information Technology
NP-Hard	Non-deterministic Polynomial-time Hard
ZKP	Zero Knowledge Proof

Chapter 1

INTRODUCTION

1.1 Overview

Ever growing instances of security breaches over the last few years has created a compelling case for efforts towards securing electronic systems and communications. The rapid growth in ecommerce applications has also made security a vital issue for many business applications. It is imperative for the success of modern businesses that cryptographic systems are deployed so that all transactions are carried out in a secure manner.

The secure transactions require secure one-to-one or group communication schemes to be deployed in an existing infrastructure. This chapter states the purpose of this research by narrating the problem statement. Furthermore this chapter sheds light on the goals that want to be achieved through this research.

1.2 Secure Communication

Secure communication refers to the necessity of providing a single platform to many users that wish to communicate securely in a collaborative fashion. This field has gained importance nowadays as the secure applications such as embedded systems, hardware fingerprinting, health care devices, smart phones and security critical systems require secure communication. The healthcare organizations hold highly sensitive data and maintaining security of this data is a challenging task. A recent article published in 2013, based on the statistical research conducted by IBM sheds light on the causes of data breaches in the healthcare organizations [1]. The details can be seen in figure 1.1.

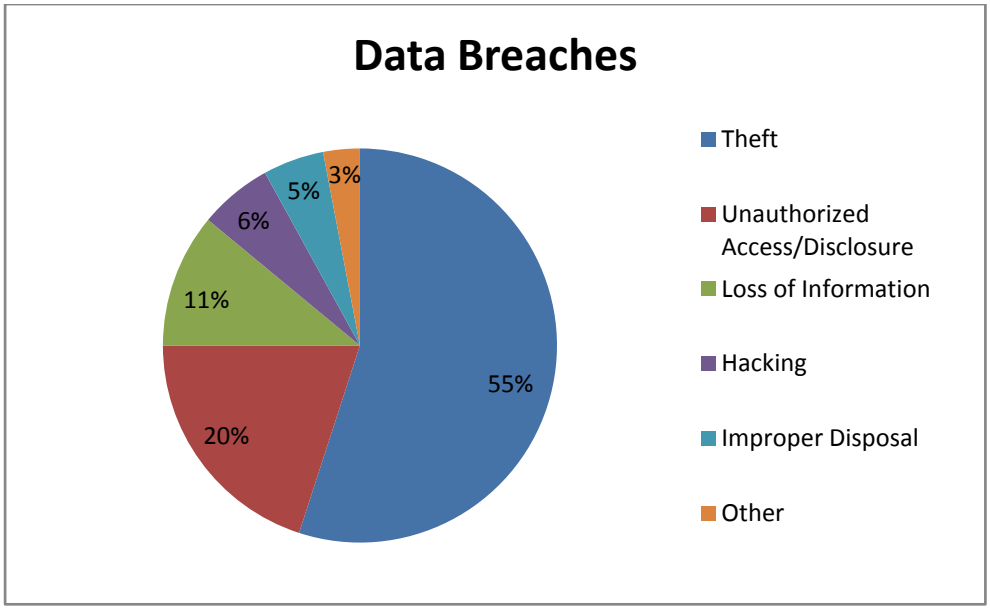

Figure 1.1: Common Causes of Data Breaches [1]

Therefore in order to avoid theft or forgery of data, proper secure communication frameworks are required that follow the CIA triad.

1.3 Major Concerns of Secure Communication Schemes

This section narrates the essentials of any secure communication scheme. The following points are of great concern while developing a secure, efficient and effective cryptosystem that is to be deployed in a dynamic environment in order to facilitate secure communication **[2]**:

- Confusion and Diffusion: All of the data related to the keys should ensure confusion and diffusion i.e. an adversary should not be able to derive any or minimal information related to the keys or the data being transmitted between the participants even if the data or server is compromised.
- Forward Secrecy: The scheme should guarantee confidentiality by ensuring forward secrecy i.e. a participant that is no longer part of a communication should no longer have access to the communications, data and keys.

- Backward Secrecy: The scheme should also ensure backward secrecy. Backward secrecy is a term that refers to the non-availability of previous data to the new participants entering the communication.
- Scalability: Scalability in a group communication environment is of great concern as the number of participants can range from a few to several hundred hence the scheme should be scalable. The scheme should be able to efficiently (timely without resource demand) manage secure multiparty communication.
- Interoperable: The scheme should exhibit the ability that it can be deployed onto existing systems/ infrastructures with minimum or no changes.

1.4 Motivation

Previous work was geared towards secure one to one communication which is a decentralized approach and the communication can be initiated by either party. In one-to-one communication schemes cryptographic keys need to be shared prior to the commencement of communication or during communication. Hence a major concern for this environment is mutual authentication leading to secure key exchange between the parties. Protocols have been developed that facilitate communication, key generation and key exchange. With the advent of high speed networks and sophisticated communication devices, interest has shifted from the conventional one-to-one communication towards group communication. Latest trends demand focus on the designing of cutting edge cryptographic schemes and protocols that facilitate in effective and efficient secure group communication.

Group communication refers to an environment where persons from different geographic dispersion communicate with each other. Since a group holds variable number of participants hence it is more prone to attacks as any person can join or leave the group at any point in time. To fully administer and control a group the

centralized approach for secure key management and key distribution is recommended which on its own is an extremely challenging activity.

There are several large scale domains where secure communication is necessary and widely applicable such as banking, teleconferencing, satellite communications, healthcare etc. These domains require client authentication, data confidentiality, integrity and availability for which state of the art schemes need to be designed. The domain specific schemes are focused towards high entropy key generation, secure distribution of keys and effective management of the keys. But these tasks become a lot more tedious and challenging in a resource constrained environment. This research is focused towards the secure communication in a resource constrained environment for which appropriate key generation and storage schemes have been brought under discussion.

The advancements being made in the field of science and technology have not only aid communication but have also produced advanced and intelligent attackers. This makes organizations desirous of highly secure communication schemes. Although new protocols are regularly proposed and previous protocols are fine-tuned on a regular basis, still constant effort is needed to ensure that we are one step ahead of attackers.

The performance of communication schemes is also crucial. Slow running cryptographic algorithms translate into consumer dissatisfaction and inconvenience. On the other hand, fast running encryption can mean high product costs. In addition to performance requirements, guaranteeing security is still a formidable challenge. Even the most secure cryptographic systems cannot provide 100% security against an adversary and are prone to attacks.

1.5 Problem Statement

Security of communication protocols has always relied on the stored encryption/decryption keys. The stored keys can be compromised therefore a framework is required that assists in the generation of keys at runtime. ICMetric technology can serve the purpose but the short length, low entropy and confidentiality of the ICMetric basis number poses a severe concern to the security of the system thereby making it a threat for use with security applications.

1.6 Objectives

The aim of this research is to design two state of the art cryptosystems that facilitate symmetric one-to-one and group communication. These two frameworks will be a collection of schemes that form a secure cryptosystem. The schemes will provide mechanism for secure admission control, increasing the length and entropy of ICMetric keys, ICMetric based symmetric key generation, mutual authentication of devices and message integrity. Furthermore incorporating the ICMetric technology in these frameworks will strengthen the security of communicating entities and the data.

1.7 Research Methodology

This research is an outcome of a threefold process. The first step is based on studying the ICMetric technology in detail and understanding the advantages of its application in the encryption/decryption schemes. The second step is to design and implement the cryptographic schemes for the secure one-to-one and group communication. The last step is to discuss the feasibility of the schemes in a resource constrained environment by analyzing their computation cost and performing a security analysis of the schemes.

1.8 Thesis Organization

In summary, this thesis presents the secure symmetric cryptographic schemes to communicate securely. The thesis has been divided in to two major modules. The first module presents a symmetric one-to-one communication scheme whereas the second part of the thesis discusses the symmetric group communication scheme in detail. Both the frameworks are based on the utilization of the ICMetric technology.

In the next chapter a detailed overview of related concepts and techniques has been presented. Chapter 2 also gives a detailed overview of related concepts and salient features of the ICMetric technology. ICMetric basis number generation is also explained in detail. In chapter 3 the frameworks for the secure one-to-one and group communication have been introduced. In chapter 4 the threats, countermeasures and the likelihood of occurrence of the threats associated with the target schemes have been presented. In chapter 5 the performance of the target schemes has been analyzed and the computational costs of the target schemes has been evaluated by interpolating the data and smoothening it with the mechanism of curve fitting. The chapter 6 concludes this research by stating the future work and effectiveness of the ICMetric based secure communication schemes in a resource constrained environment.

Chapter 2

LITERATURE REVIEW

2.1 Overview

ICMetric refers to a postmodern technology that can be used to extract measureable and unique attributes from the hardware and software environment of a system. The technology exploits the fact that each device is unique in its internal environment therefore the factors that make each device different can be used to generate a single and unique number for every device. A brief overview of the work performed on the ICMetric technology has been presented in this chapter. This chapter also focuses on the possible advantages of utilizing the ICMetric technology in the formation of secure communication schemes. Furthermore the work done related to the secure communication is presented in this chapter in detail.

2.2 Encryption Techniques

Encryption is the most important component of any secure communication protocol. The aim of encryption is to hide the data from an adversary during transmission in order to ensure privacy and secrecy of the data. The plain text after being encrypted is termed as cipher text. Once the transmitted cipher text is received by the recipient it is decrypted to uncover the underlying plaintext. There are mainly two techniques for encryption based on which the encryption protocols are designed. The first technique is called Symmetric encryption whereas the other technique is Asymmetric encryption. These techniques differ mainly in the keys being used for the encryption/decryption. Both of these techniques are discussed below:

2.2.1 Symmetric Encryption

This is the oldest and best known technique used for the encryption of data. The classical cryptographic protocols are based extensively on the utilization of this technique for developing secure communication protocols. A secret is required to be shared among the communicating parties prior to the communication. Identical keys are used for the encryption and decryption of the data. The key can be a simple number or can be derived from an already communicated mathematical function. Until both the sender and recipient have the common shared keys, the secure communication can be achieved. The figure 2.1 gives a generalized view of the symmetric encryption in secure communication

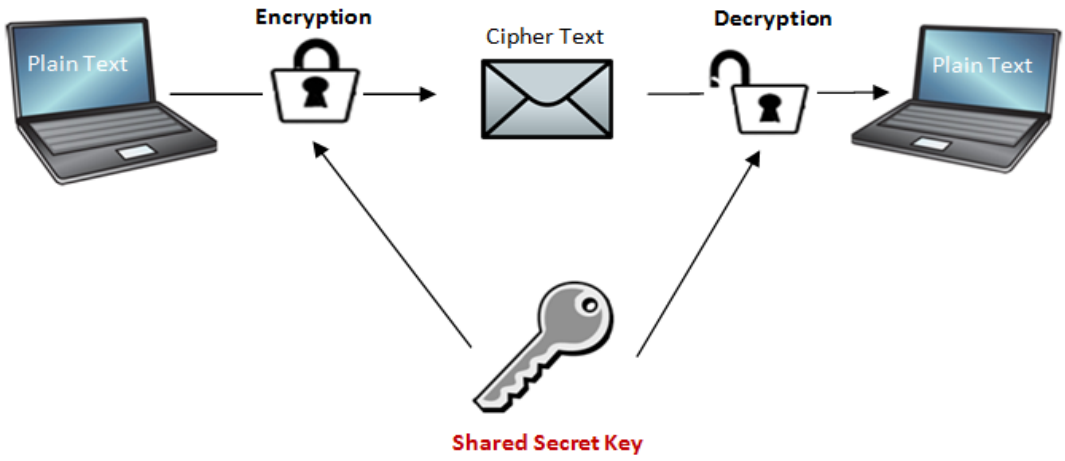

Figure 2.1: Symmetric Encryption

2.2.2 Asymmetric Encryption

In asymmetric encryption each entity is associated with two different but related, public and private keys. The encryption is done with the help of the public key associated with the recipient. Once the cipher text is received the recipient can uncover the underlying plaintext by decrypting it with his private key. The private key is known only to the recipient himself and kept secure/ secret from any other

communicating party. Figure 2.2pictorially represents the asymmetric encryption technique.

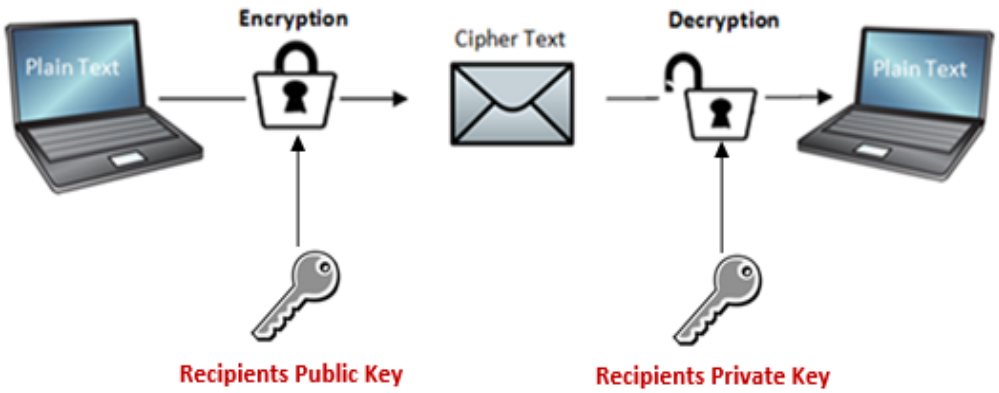

Figure 2.2: Asymmetric Encryption

2.3 Secure Communication Environments

The encryption schemes may vary depending upon the environment where the secure communication is to take place. These environments range from two party communication to multiparty communication. These environments are specified as one-to-one and group communication environments. These environments need to be considered in secure communication because the effective and efficient communication is dependent upon it. Both of these environments are briefly discussed below:

2.3.1 Secure One-to-One Communication

One-to-one communication also termed as peer-to-peer communication is a special type of communication network in which both the communicating parties have resources of their own. This type of communication model mostly uses a decentralized approach. The communication takes place between two communicating entities only.

Since this model uses a decentralized approach it is more susceptible to attacks. Furthermore since there is no authority or administrator to observe the communication therefore authenticating the participants can be a challenging task. Some of the attacks possible on this types of communication network are

- Denial of Service (DoS) Attack
- Network Poisoning
- Man in the Middle attack
- Injection Attack

These types of attacks can be prevented by encrypting the one-to-one communication traffic so that the transmitted data even if spoofed by an adversary will not convey any meaningful information. Therefore encryption of the transmitted data can help in mitigating the possibility of insertion attacks. Therefore if the symmetric/asymmetric keys are known to both the peers prior to the communication, the encrypted data can be transmitted and the possibility of the attacks can be narrowed down.

2.3.2 Secure Group Communication

Group communication is an environment where several participants intend to communicate with each other securely. This type of an environment requires the assistance of a group controller or key distribution manager so that the keys can be distributed among the communicating parties. Furthermore the group controller is also responsible for managing the admission and exclusion of the participants. The rekeying is also required whenever a participant enter/leaves the group communication. Hence ensuring security in group communication is a more difficult and challenging task. Following are some of the probable attacks on group communication environments

- Injection Attack
- Denial of Service (DoS) Attack
- Interception
- Man in the Middle Attack

2.4 ICMetric Technology

ICMetric [3] is a novel concept in the field of cryptography. Conventional cryptography relies on the storage of cryptographic keys on the system i.e. the keys are stored either at the client's side or at the server's side. A compromise in keeping the keys secure can result in a security breach. Suppose that the cryptographic keys are stored on the system, if the system is compromised it will result in the failure of the entire security framework. To resolve problems related to key storage the use of ICMetric technology has been proposed. Figure 2.3 shows the flow of events that are followed for the cryptographic key generation in an ICMetric based cryptosystem.

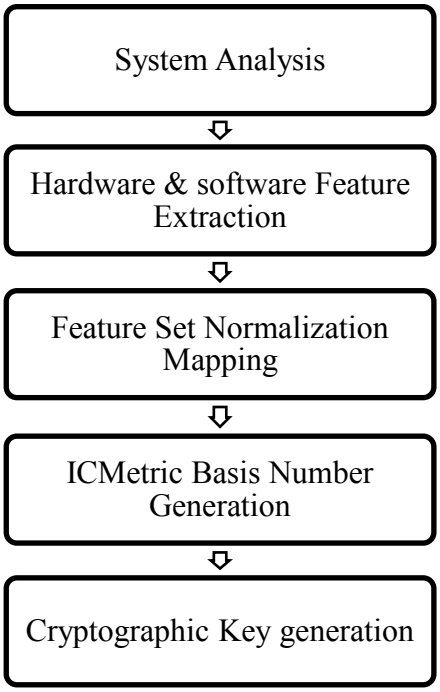

Figure 2.3: Flow of events for ICMetric based Cryptographic Scheme

By using the ICMetric technology a system can generate a basis number. A basis number is a dependent upon the system properties. Hence the basis number generation requires prior system analysis so that appropriate hardware and software features can be extracted. The individual features are extracted by considering correlations between features, probability analysis, complexity analysis and feature profiling. Probability analysis is based on the statistical analysis i.e. the possible values within which a feature's value can occur. Complexity analysis involves the identification of practicality in order to generate the features. Feature profiling does a behaviour analysis that mentions and simulates how a feature performs in certain condition. Based on this analysis the features are extracted. Once the features are extracted the ICMetric technology uses these specific hardware and software characteristics for establishing the feature sets. Since the extracted features are static and dynamic therefore a feature exhibits a particular behaviour. Therefore standard deviation analysis is to be performed that identifies the deviation of the feature from the normal value. This process is called as feature normalization mapping. The normalization mapping is applied to form an acceptable range in which the values are considered acceptable.

2.4.1 Salient Features of ICMetric Technology

ICMetric is a postmodern security technique that promotes the use of unique system attributes/features to generate a unique identification number termed as the ICMetric basis number that can then be used to generate secure cryptographic key(s). A unique property of the ICMetric technology is that if any attempt is made to compromise the system then it will result in the generation of an inaccurate ICMetric number because the features are extracted from the hardware, software, environment and user characteristics. Any tempering done with the system will change the values

of the respective features. Also the number cannot be extracted/compromised since it is never physically available on a system and can be regenerated when required. An ICMetric number must possess the following properties to ensure the highest levels of security:

- Diverse – The ICMetric number should uniquely identify every computation device.
- The ICMetric number should be generated without human intervention.
- The ICMetric number should be generated upon requirement and discarded thereafter.
- The ICMetric number should be non-predictable and hence non generateable by an attacker.
- Stable – for the owner an ICMetric number should be re-generateable i.e. if no change has been made to the device then the same ICMetric number should be generated.
- No single or group of persons should be able to extract a particular device ICMetric number by using the ICMetric algorithm.
- No need to store any template (as for the biometric validation) that can serve the purpose of validating the device.
- The secure cryptographic key(s) are derived from the ICMetric basis number.

The ICMetric number, cryptographic keys or any information related to the ICMetric number is not residing on the system, thereby reducing the probability of key theft and impersonation based attacks. Furthermore the ICMetric number is generated and discarded after use. ICMetric technology also ensures non repudiation of data because a particular ICMetric number can only be generated by the relevant

entity and as a result the data sent associated with the ICMetric number cannot be denied.

2.4.2 ICMetric Basis Number Generation

The selection of features is a critical task because inappropriate feature selection will result in poor system security. Traditionally device fingerprinting has relied on only using device features like the MAC address. The problem with using features like the MAC address is that it can be spoofed. Hence to ensure fool proof security the ICMetric system needs to be based on characteristics that cannot be predicted or reproduced. This is precisely why the ICMetric technology relies on using device features and behaviors to generate a unique identification for the device.

To highlight the problem associated with feature selection, consider two smart phones that have been manufactured by the same manufacturer and are identical to each other in all respect. If one tries to generate unique identifications for the smart phones then he is faced with the problem that there are not many distinguishing features that set apart one device from the other. To establish a unique identification for mass produced devices one must realize that generation of an identification has to rely on features that cannot be easily predicted therefore we must also consider features that are less apparent than the conventional / obvious features. While using the ICMetric technology we acknowledge that the only features which help in distinguishing between two identical smart phones are internal features for instance addresses, hardware profiles, contact lists, network profiles, minute differences in camera resolutions, sensor discrepancies etc.

Successful attempts have been made in determining features that are appropriate for the ICMetric system. A feature qualifies as a candidate for the ICMetric system if the individual feature values can be normalized because if there is

too much variation in the values then the ICMetric number will not be stable and cannot be used for the system identification. Modern smart phones and health monitoring devices are commonly equipped with sensors that possess a unique behavioral characteristic which can be used for identification. But not all sensors/ devices can be employed for this purpose. For instance every accelerometer will react differently to the same input parameters. This means that even when a sensor is at rest it will register an acceleration which is unique to that particular sensor. Normalization of these values along with calibration data results in a number which forms part of the ICMetric identification. Although this feature can assist in the generation of an ICMetric number the same is not possible for other sensors like the gyroscope or GPS sensors. To detect similar inconsistencies in gyroscopic readings the device has to be placed in an apparatus that can rotate the device at a constant angular velocity while changing the speed. The production of an apparatus with this ability is a difficult feat and is not helpful since the ICMetric number needs to be generated at run time without human intervention. Traditionally GPS devices have worked by using three satellites to determine the location of a GPS receiver using triangulation. The distance is calculated by using an inaccurate clock that determines the time it took for a signal to travel from the satellite to the receiver. Although the clock skew seems to be a useful feature for the formation of a fingerprint, it cannot be used because modern GPS receivers utilize a fourth satellite which takes into account the clock skew.

The generation of the ICMetric basis number is also performed by locating features that are correlated. Hence the generation of the ICMetric number relies on feature correlation analysis. Mathematically the generation of the ICMetric basis number requires change probability analysis, feature normalization, complexity analysis **[**4**]**. An important requirement while selecting features for the ICMetric basis

number generation is that the individual feature values should follow a normal distribution.

2.4.2.1 Methods for ICMetric Basis Number Generation

Following are the two methods by which ICMetric basis number can be formed from the selected features

- Feature Addition-Combination Technique: Once the individual features are established, the final ICMetric number ICM is represented by adding or XORing the individual features t_i. This results in the generation of a small yet stable basis number.

$$ICM = t_1 + t_2 + \cdots + t_n$$

- Feature Concatenation-Combination Technique: Using the concatenation operation the individual features are established. As a result the generated ICMetric number ICM is represented by concatenating the individual features t_i. The basis number that is generated as a result of this technique is of a longer length but lacks stability.

$$ICM = t_1 \parallel t_2 \parallel \cdots \parallel t_n$$

Once the individual feature values are established then a final ICMetric basis number can be generated by using either the feature addition technique or the feature concatenation technique. Both of the techniques are established on the extraction of appropriate features and the application of normalization maps i.e. standard deviation analysis of the feature sets in order to provide basis number stability.

After the ICMetric basis number has been generated it is used for the generation of the cryptographic keys. The cryptographic keys can be generated depending upon the underlying algorithm that is tuned in accordance with the

ICMetric technology. The cryptosystem designed as a result will generate its ICMetric number along with the keys at the runtime. Hence neither the ICMetric number nor the cryptographic keys are stored on the system.

2.5 Existing Communication Schemes

Recently secure communication has emerged as an important requirement, hence extensive research is being carried out specifically in this area of communication. Key distribution and key management is a cornerstone of all secure communication schemes. Diffie Hellman Key Exchange protocol [5] was developed to establish and facilitate secure one-to-one communication. Even though the protocol focused on the conventional one to one communication but this protocol resulted in the opening of several doorways in the field of information security. Based upon the significance of the Diffie Hellman key exchange protocol, even today this protocol is the underlying protocol for many schemes that assist in one-to-one or group communication. Owing to its simplistic design, it won't be wrong to say that even today we focus on the utilization and extension of the basic Diffie Hellman key exchange protocol that was designed mainly for the generation/management of keys for two party communications. Different alternatives have been discussed in [6][7][8][9] that mainly intend to focus on the group communication while extending the basic functionality provided by the Diffie Hellman key exchange protocols. The target schemes are either based on a centralized authority to generate the keys or the key generation is done purely at the clients end. The centralized authority is responsible for the admission control and group key generation. Reliance on the centralized approach also has its downfall, since the group becomes a single point of failure if the server side does not withstand an attack. Whereas, if the keying is done at the clients end, the dynamic nature of the group communication becomes a

challenging task and these schemes don't cater for it. In a dynamic environment forward and backward secrecy needs to be maintained and this has to be reflected in the design of the scheme itself.

In [10] a study has been conducted on the utilization of different topologies for the secure communication. Their work focuses on the use of mesh or ring topologies to facilitate secure communications. Their scheme lacks the needed level of security as they do not consider the use of a group controller. The absence of a group controller results in the lack of flexibility because the management of the group participants becomes a complex task. Similarly in [11][12] the authors have proposed that each user should be associated with a separate/individual stored key. If this concept is followed we are faced with two problems i.e. key theft and key structuring. The size of a group can grow very quickly therefore a data structure is also recommended that helps in the secure storage of the keys. This data structure compliments the process of key generation, management and storage but lacks in providing high level security as these schemes are prone to insider or outsider attacks. As a result the target schemes cannot be used in resource constrained environment. The probability of attacks increases as the keys are being stored on the system and these keys can be exploited by an adversary.

Lai et al. in [13] have proposed *BROSK* (BROadcast Session Key negotiation protocol) for the secure communications among a number of nodes that form a wireless sensor network. With *BROSK* every node broadcasts a message containing its nonce. So, every two neighbouring nodes that hear each other can compute a common key which is function of their two nonce. Neighbouring nodes authenticate themselves with a redeployed key which is supposed to be unreachable in case the node is captured. A variation [14] of this protocol has also been proposed in which the

redeployed key is used only for a restricted period of time. The nodes participating in the secure communication establish pair wise keys. Once the nodes have communicated, the key is erased thereby preventing key capture by an adversary during storage. However, a “Hello” message is used to establish pair wise keys and is sent in the clear. So, an attacker can spoof a node and also eavesdrop the hello messages. As a result the adversary can use the IDs and nonce’s contained in these messages to derive the established keys and hence the entire scheme can be compromised.

Modern research focuses on using the device fingerprints in designing schemes for secure communication cryptosystems. Xu et al. in [15] have discussed in detail the challenges and opportunities based on the use of device fingerprinting in wireless networks. The concept of involving device features in communication cryptosystems is not new; rather it dates back before the start of World War II [16]. With the passage of time information security gained importance and with the reliance on high end computing devices the involvement of device fingerprinting has been proved to be significant enough to be studied widely. Uptil now schemes were being developed that relied upon stored cryptographic keys. The theft of the stored keys caused several challenges. Hence researchers introduced the generation of encryption keys from electronic circuits. The electronic circuits caused several issues among which the stability of the cryptographic keys was the biggest issue. Different keys were generated every time the communication started due to which this scheme couldn’t come under the spotlight. So this proves the fact that researchers have attempted to involve device characteristics in key generation from the very beginning. Nowadays systems use digital circuitry based on high speed processors, memories, hard drives, sensors etc. so the digital system characteristics can be used in

cryptosystems for the key generation. Here one would argue that if two devices have the same specification then same keys will be generated for both devices. Even if two computation devices possess the same hardware and software resources they will differ on low level characteristics. Low level features include but are not limited to MAC addresses, identification numbers, IMEI, addresses, files that exhibit frequent user behaviour etc. It is these low level features that set apart one device from the other.

Integrated Circuit Metric or ICMetric technology exploits the different hardware and software features of a system to produce an ICMetric basis number that is unique to the system. The ICMetric technology can be closely related to the Biometric technology. Biometrics help to identify humans uniquely based upon their body features, properties and behaviour; whereas ICMetric helps identify a system uniquely based upon the system features.

ICMetric is a technology that has been developed based on the principles of information security and incorporates digital system characteristics for key generation. Latest work in the field of cryptography advocates the use of device features also termed as device fingerprints for the generation of system keys. In [4] the authors have discussed the properties of the ICMetric technology in detail, where they also discuss the mechanism behind selection of appropriate features for the ICMetric system. Zhai et al. in [17] have briefly discussed the applications of ICMetric technology and the extraction of appropriate features that can be used in developing secure embedded and healthcare systems.

Papoutsis in his extensive work [18] proves that ICMetric technology has the potential of being used for the generation of encryption keys. The author discussed the viability of using the ICMetric technology for the generation of a system

identification and then for the generation of encryption and decryption keys. The methods that can be used to generate keys using the ICMetric technology have been discussed in detail in [19]. His extensive work explains how ICMetric can be used to reduce the potential security risks in many embedded system environments. The author has extended his research to enumerate the advantages of using ICMetric in cryptosystems for the key generation over the conventional key generation schemes. In his work he also explains which features need to be considered and how particular data sets are chosen to generate a single but unique ICMetric number. The author has also performed a detailed analysis of the ICMetric technology while keeping the strengths and weakness of this technology under consideration. Kovalchuk et al. in [20] have discussed the advantages of using the ICMetric technology in resource constrained embedded systems.

Further work [21] has resulted in the creation of a scheme for the generation of an asymmetric key using the ICMetric key. To provide strength the authors have also incorporated techniques for key stretching and the entropy of the keying system. Along with secure key generation and management the protocol ensures confidentiality and availability of the data.

Various experiments have proved that the ICMetric technology can be adopted in many domains of computing. A study on ICMetric and autonomous healthcare systems [22] proves that healthcare systems need to be secured and that ICMetric can fulfill the individual security goals required by these special embedded systems. ICMetric technology has been studied on an intelligent wheelchair [23] that uses the ICMetric number to secure the communications of the mobility device. Besides this the use of ICMetric technology has also been proposed in technologies that link

security and cloud computing [24][25]. The security issues and potential solutions by using ICMetric based encryption in cloud computing are discussed in detail in [26].

2.6 Summary

In this chapter, a literature review of the ICMetric technology has been provided. This chapter starts with discussing the major concerns while developing a secure communication cryptosystem. The secure communication environments i.e. one-to-one communication and group communication environments are discussed in detail. The salient features of the ICMetric along with its different areas of application have been discussed. The ICMetric number generation is a challenging task as it requires close analysis of the system features. This chapter gives a good understanding of the ICMetric basis number generation. Towards the end of the chapter, already published communication schemes have been discussed and analyzed. This existing work sheds light on the advancement made in the field of information security over the past several decades up till now.

Chapter 3

PROPOSED SECURE COMMUNICATION FRAMEWORKS

3.1 Overview

With communication comes the challenge of secure communication. Secure communication is a collaborative environment where users intend to communicate securely. All of the communication data is secured by encrypting it with the help of cryptographic keys. Secure communication can be used in the secure one-to-one and group communication environments. Both of these environments have challenges of their own that require secure communication frameworks deployed prior to the communication. This chapter proposes secure one-to-one and group communication protocols based on the utilization of the ICMetric technology. The chapter discusses the protocols in detail.

3.2 Secure One-to-One Communication Protocol (SOCP)

Secure one-to-one communication is a distributed architecture that focuses towards the communication between two entities. The security in a distributed and decentralized environment can be termed as an extremely challenging task for which a state of the art framework is required. SOCP is designed particularly for this environment. SOCP is a symmetric framework that incorporates the ICMetric features and comprises of several schemes tuned in accordance with the ICMetric technology [**27**]. The schemes provide secure mechanisms for secure admission control, key generation, mutual authentication, encryption/decryption and message integrity. Whenever a person intends to communicate he has to register himself with the server.

This helps in the process of key generation. Now both the parties i.e. the server and the client have to generate symmetric session keys in order to send encrypted data to each other. Now both the parties have to ensure that they possess the same session keys for which both have to authenticate one another. The message integrity and encryption/decryption both go side by side. These schemes collectively ensure secure communication among the participants. The following subsections discuss these modules in detail.

3.2.1 System Model

The proposed scheme is an idea for networked entities and all devices forming part of the network have trust in the server. The server is responsible for controlling all the entities in the network and therefore enables devices to establish a trusted relationship between them. This trusted relationship enables entities that have never had contact to carry out interaction securely and confidentially. We make the following assumptions in the design of our proposed schemes:

- Each entity that is part of our network is registered at the server. This registration is done before the actual communication takes place.
- The server is also responsible for assigning all network specific configurations to all the registered entities that form part of the network.
- The registration of an entity requires manual as well as electronic data collections.
- All entities already trust the server before proceeding for the secure communication based on our protocol. This trust has been established without authentication or with authentication using a side channel such as SSL or manual registration.

3.2.2 Admission Control Scheme

Suppose that a client 'A' wants to communicate with the server 'S'. In order to join the network, the client 'A' has to register itself with the server. The client's registration is a onetime process. This process is initiated when the client requests to register with the server by supplying all the required credentials. The client and server jointly select some public perimeters termed as g and n, where g is the generator, n is a prime number. These public parameters are the preliminaries to the secure one-to-one communication protocol. These parameters are to be selected after mutual discussion between the communicating parties prior to the session establishment.

After selecting the public parameters, following steps are to be followed for the admission control:

Step 1. The client 'A' generates a verifier (v) based on the discrete log problem

$$v = g^{X_A} mod\ n$$

where X_A is the ICMetric number of client 'A'

Step 2. The verifier (v) is sent to the server. The server stores the client's id, salt and verifier. The salt is a random number generated by the server. Once the entity is registered, the server assigns a unique identification number and a 128 bit random salt value.

This salt value aims in increasing the entropy of the ICMetric basis number and safeguards our scheme from the possibility of launching pre-computed attacks. Furthermore the salt value also helps in ensuring confusion and diffusion among the data being transmitted because the attacker cannot deduce any keys from the data being transmitted.

3.2.3 Key Generation Scheme

This process requires the generation of the symmetric keys. The client 'A' contacts the server 'S' requesting the session keys. Following tasks are performed for the key generation:

Step 1. The server 'S' responds by sending the client 'A' his respective salt. Once the salt is received the client performs the following operation to generate a random number a

$$a = H(X_A \parallel Salt_A \parallel Id_A)$$

where $H(\,)$ is a one way hash function i.e. a variant of SHA-2. $\parallel$ represents the concatenation of variables.

Step 2. Now the client computes A and sends the result to the server

$$A = g^a mod\ n$$

The following step onwards uses the Secure Remote Password (SRP) protocol. The use of SRP protocol is very suitable for this framework because it allows a device to authenticate itself to a server without exchanging the shared secret key or any private information.

Step 3. The server upon receiving A does the following calculations

$$b = H(X_s \parallel Salt_s \parallel Id_s)$$

$$K = H(g \parallel n)$$

Where $X_s, Salt_s, Id_s$ is the Server's ICMetric number, Salt and Id respectively.

Step 4. Based on the calculation made in step 3, the server calculates B and sends the result to the client

$$B = (Kv + g^b) mod\ n$$

Both sides i.e. client ‘A’ and server ‘S’ have A and B so as a result u can easily be computed as follows

$$u = H(A \parallel B)$$

3.2.3.1 Session Key Generation

Since the desired calculations have been done that are required in the session and symmetric key generation. Now the client ‘A’ and server ‘S’ generate the cryptographic keys.

The client ‘A’ constructs the session key as follows.

$$S_A = (B - Kv)^{a+uX_A} mod\ n$$

$$= (Kv + g^b - Kv)^{a+uX_A} mod\ n$$

$$= (g^b)^{a+uX_A}$$

The client’s session key is

$$K_A = H(S_A)$$

The server constructs the session key K_s as follows

$$S_s = (A.v^u)^b$$

$$= (g^a.g^{X_s(u)})^b$$

$$= (g^b)^{a+uX_s}$$

The server’s session key K_s is

$$K_s = H(S_s)$$

3.2.4 Authentication Scheme

Both the client ‘A’ and server ‘S’ need to prove that they possess the same session keys. To do this both the parties will generate messages that will help authenticate each other.

3.2.4.1 Client's Authentication

Firstly the client authenticates itself by generating the following message and sending the result to the server

$$M_1 = H(n \parallel g \parallel Id_A \parallel Salt_A \parallel A \parallel B \parallel K_A)$$

Now server does a similar computation

$$M_2 = H(n \parallel g \parallel Id_a \parallel Salt_A \parallel A \parallel B \parallel K_s)$$

If $M_1 = M_2$ then the client is authenticated otherwise the client may be termed as an adversary.

3.2.4.2 Server's Authentication

Now the server authenticates itself by generating the following message and sending the result to the client

$$M_3 = H(M_1 \parallel A \parallel B \parallel K_s)$$

Now client does a similar computation

$$M_4 = H(M_1 \parallel A \parallel B \parallel K_A)$$

If $M_3 = M_4$ the server is authenticated otherwise the client may declare the server an adversary.

3.2.5 Encryption/Decryption Scheme

The encryption and decryption is based on the use of Advanced Encryption Standard New Instructions (AES-NI). AES-NI is a CyaSSL embedded library **[**27**]** that can be used for implementation in a resource constrained environment. The symmetric keys (K_A and K_s) generated in the key generation phase are used for the process of encryption/decryption.

3.2.6 Integrity Scheme

The encryption / decryption and message integrity check both go side by side. The aim of data integrity is to prevent unintentional changes to the data and information.

Now suppose the server wants to check the integrity of the message 'M' that is sent by the client.

The client performs the following tasks:

Step 1. The message M is passed through the one-way hash function $H(\,)$. The hash function would be a variant of SHA-2 and same as used in the key generation scheme

Step 2. The obtained hash is concatenated with the original message. The resulting message is called P

$$P = M \parallel H(M)$$

Step 3. Now P is encrypted with AES using the Session Keys generated previously and the result R is sent to the server.

$$R = E_{K_A}(P)$$

The server now performs the following tasks:

Step 4. The server now decrypts the transmitted result R with his symmetric session key to uncover the message M and message hash $H(M)$

$$R_1 = D_{K_s}(R)$$

So now

$$R_1 = M \parallel H(M)$$

Step 5. The server now calculates the Hash of obtained message M using the same one-way hash function.

Step 6. If the calculated hash $H_1(M) = H(M)$, the integrity is intact otherwise the message has been changed by an adversary during transmission.

3.2.7 Complexity Analysis

ICMetric technology on its own has the ability to be used in a resource constrained environment because the ICMetric number generation consumes very less resources [20]. Apart from the advantages of the ICMetric technology, for any scheme to be deployed in a resource constrained environment the asymptotic analysis is performed. One thing to consider is that there should be a balance between the complexity and level of security provided by a framework. Therefore the next step is to perform a complexity analysis of our scheme.

Our proposed protocol uses SHA-2 (256) in the key generation, authentication and integrity schemes. SHA-256 uses a block size of 512 bits and iterates 64 rounds. The complexity for a single block is O(1) but for several blocks it is O(M) where M is the total number of blocks.

For the complexity analysis of AES on a fixed block size of 256 bit key and 14 rounds the asymptotic analysis yields that it is independent of the input therefore AES is O(1). In order to encrypt longer messages (M), the complexity becomes O(M) because O(M) blocks have to be encrypted.

3.3 Euclidean Based Group Communication Protocol (EGCP)

ICMetric can be used in dynamic environments where large numbers of participants intend to communicate securely. ICMetric has the advantage that it can facilitate various forms of communications while ensuring the highest levels of security. A problem with keys is that they can be captured which results in security compromise. ICMetric improves system security without reliance on keys stored by

the group controller, Key Distribution Manager (KDM), server or the participant. Hence whenever a participant leaves or enters the group new keys are generated. In this section a group communication protocol has been developed that is an extension of the protocol introduced in [28]. Our proposed protocol incorporates ICMetric technology for the cryptographic key generation and as a result provides greater security and attack resilience based upon the properties of the ICMetric technology.

3.3.1 System Model

The proposed scheme is an idea for networked entities and all devices forming part of the network have trust in the server. The server is responsible for controlling all the entities in the network and therefore enables devices to establish a trusted relationship between them. This trusted relationship enables entities that have never had contact to carry out interaction securely and confidentially. We make the following assumptions in the design of our proposed schemes:

- Each entity that is part of our network is registered at the server. This registration is done before the actual communication takes place.
- The server is also responsible for assigning all network specific configurations to all the registered entities that form part of the network.
- The registration of an entity requires manual as well as electronic data collections.
- All entities already trust the server before proceeding for the secure communication based on our protocol. This trust has been established without authentication or with authentication using a side channel such as SSL or manual registration.

3.3.2 Participant Admission

To facilitate group communication a participant must gain acceptance to the group by following an admission process. Following steps are followed when a participant joins the group communication:

Step 1. Suppose there are i participants/members willing to communicate securely

$$M_1, M_2, \cdots, M_i$$

Step 2. Every participant registers itself with the KDM. KDM allocates an ID to each participant along with its own public key.

Step 3. Each participant M_i generates his ICMetric basis number, denoted by ICM_i

Step 4. Every participant M_i generates R a random number, equal in length to his ICMetric basis number (ICM_i) i.e. R_i

Step 5. Now every participant XORs the random number (R_i) with the ICMetric basis number (ICM_i)

$$X_i = ICM_i \oplus R_i$$

This step helps increase the entropy of the ICMetric number and the key being generated

Step 6. Each member M_i encrypts X_i with the KDM's public key.

$$Y_i = E_{KDM_{Pub}}(X_i)$$

Step 7. The KDM decrypts each Y_i with its private key.

$$Z_i = D_{KDM_{Priv}}(Y_i)$$

Step 8. KDM selects a random number $K > Z_i, \ \forall i$. That is

$$K > Z_1, K > Z_2, \cdots, K > Z_i$$

Step 9. The KDM computes integers a_i, b_i and generates a message $(a_i, b_i), \forall i$ and transmits the message (a_i, b_i) to all the associated participants M_i. Where

$$a_i = K/Z_i$$

$$b_i = K \bmod Z_i$$

Step 10. Each participant M_i calculates the group's key by computing the Euclidean Algorithm

$$k = a_i * X_i + b_i$$

Where k is the generated session key. Now every participant can send the message after encrypting it with the session key whereas the receiver can decrypt it with the same session key. The proposed scheme can be scaled to facilitate large number of participants and can be implemented in a resource constrained environment.The strength of the scheme lies in the use of ICMetric technology and the Euclidean Algorithm. Figure 3.1 gives a pictorial representation of the proposed scheme in the form of a flowchart focusing on the key generation process for the better understanding. The key (k) is a session key can be generated by each participant independently.

The strength of the designed protocol lies in the fact that the ICMetric number is XORed with a random number, it causes diffusion and prevents the ICMetric from direct exposure while it is being transmitted. Secondly the number generated as a result of the XOR is transmitted securely over the network using any of the public key infrastructures that adds another layer of security to the basis while it is being transmitted.

The key formation is done by the client/participant and is based on the message *a* and *b*. The values that are derived from the message are used in the Euclidean Algorithm. Thus even if an attacker gets hold of the message and he doesn't know the number Z_i (generated based on the ICMetric number), as a result he can't calculate the key. Furthermore X_i can never be captured by an adversary. This strength is called an NP Hard problem **[**29**]** i.e. the adversary can neither deduce nor capture the ICMetric number X_i even if the messages are

spoofed. The greater the entropy of the keys the difficult it is to deduce any information from the data transmitted, which also narrates the security of our algorithm.

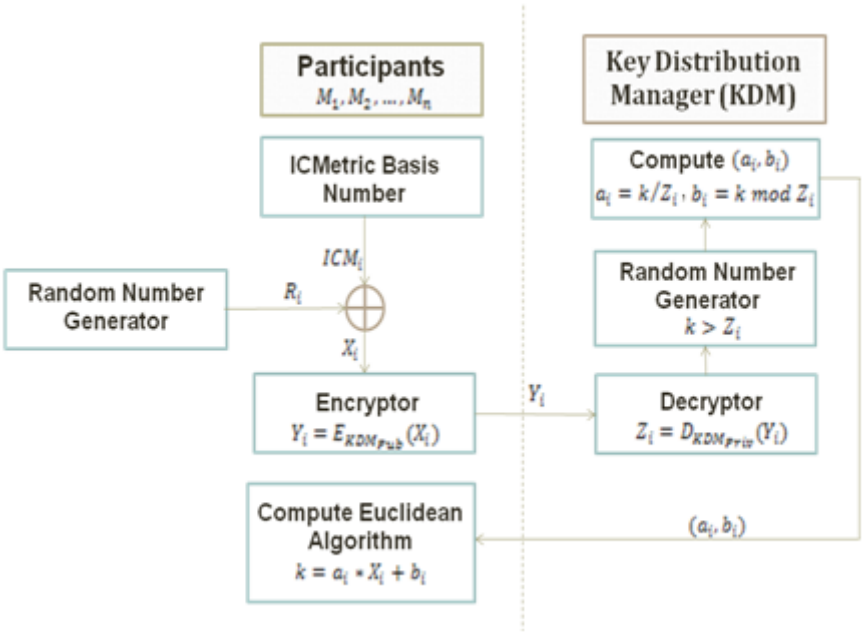

Figure 3.1: Flow of events for EGCP

3.3.3 Participant Exclusion

When a participant leaves the communication or as prescribed by the policies followed by the organization (where the protocol is being deployed) the rekeying procedure is followed by the KDM. The rekeying is performed by undertaking the same process which was followed when the participant joins the group. The only exception at this stage is that the participants do not have to register themselves with the KDM. With the help of the rekeying process the scheme assures forward secrecy, backward secrecy and key freshness.

3.3.4 Complexity Analysis

In order to check the feasibility of our proposed protocol, an extensive complexity analysis in terms of time consumption/number of computations and security analysis is to be performed. The asymptotic analysis of our protocol for a key

size of 256 bits yields that our protocol shows O(1) complexity for the clients tasks. Whereas the KDM shows a complexity of O(1) for one participant and O(M) for M participants intending to communicate securely. Based on this fact, our protocol can be deployed in a resource constrained environment.

3.4 Summary

This chapter introduces the secure communication frameworks based on ICMetric technology. The chapter is divided into two parts. The first part introduces the Secure One-to-One Communication Protocol (SOCP). The admission control, key generation, authentication, encryption / decryption and message integrity schemes related to SOCP are discussed in detail. The second part of the chapter discusses the Euclidean based Group Communication Protocol (EGCP). The participant admission, Key generation and exclusion aspects are introduced for EGCP. Both of these frameworks are based on symmetric keys.

Chapter 4

SECURITY ANALYSIS

4.1 Overview

Secure communication relies solely on secure generation, management and storage of the cryptographic keys. Advancements in technology and security have caused attackers to become more and more sophisticated. It is understood that no scheme can provide a comprehensive solution against all possible attacks. Hence to design an optimum cryptosystem a close analysis of the possible attacks on the framework needs to be done.

This chapter presents an attack model that discusses the possible attacks on our proposed frameworks. The threats and countermeasures associated with the target schemes have been presented. Possible effects of the attacks has been discussed where appropriate countermeasure are not applied.

4.2 Attack Model

The possible and significant attacks need to be identified in order to visualize the possible effects on the frameworks. In **[**30**]** the author has listed all the attacks that are possible on an embedded system. Out of the list, the attacks relevant to the secure communication have been selected. This section discusses the possible adversary attacks on the Secure One-to-One Communication protocol (SOCP) and Euclidean based Group Communication Protocol (EGCP). Figure 4.1 illustrates a scenario where attackers are performing different attacks to effect the secure communication among the communicating devices. The attacks mentioned in the figure 4.1 are discussed in detailed in the proceeding subsections

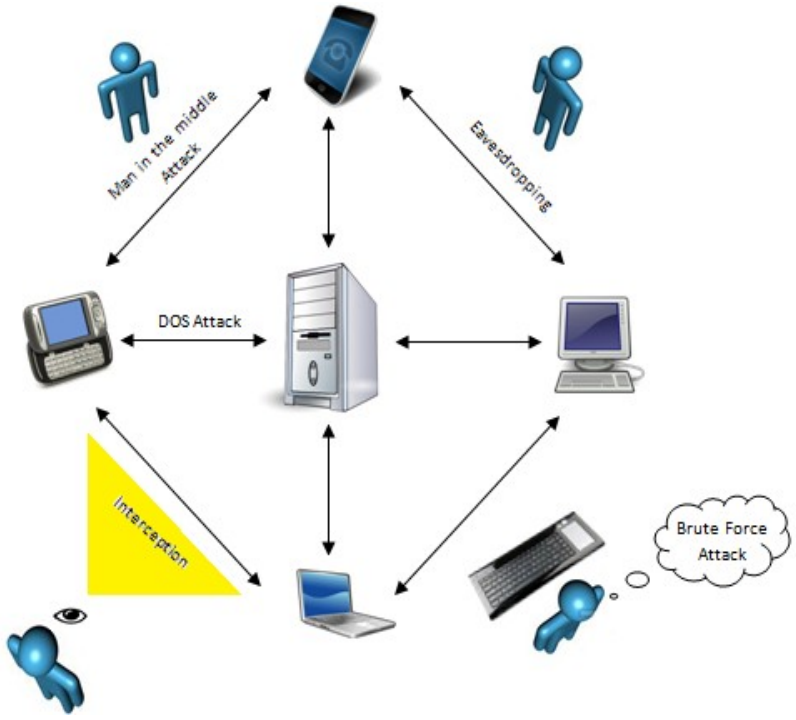

Figure 4.1: Adversary Attacks on Secure Communication Frameworks

One thing that is to be kept under consideration is that our schemes effectively coveys a Zero Knowledge Proof (ZKP). ZKP is a method using which a prover can prove to the verifier that a given statement is true without conveying any information other than the fact that the statement is indeed true. ZKP property is particularly in lined with the use of ICMetric technology in our designed framework. The ICMetric number cannot be transmitted over the channel and ZKP helps preserve this property of ICMetric technology. Using ZKP in our scheme we were able to prove to the server about the knowledge of ICMetric through mathematical computations.

4.2.1 Brute Force Attack

Brute Force attack is an exhaustive attack in which all the possible key combinations are tried by an adversary until the true cryptographic key is identified within polynomial time **[**31**].** The easiest way to prevent brute force attack is that the designed scheme should generate keys of a sufficient length and entropy so that the

attacker fails to guess the keys in polynomial time. Both of the target schemes (SOCP & EGCP) incorporate countermeasures against the brute force attack as they increase the entropy and length of the keys. Furthermore owing to its unique design the key is generated from the ICMetric basis number that comprises of many system features that cannot be guessed by an adversary. The length can be kept variable according to the need of the schemes employed. Secondly the cryptographic keys are generated at run time and discarded after use, this makes the task of an adversary even more difficult because the keys last only for a particular session.

4.2.2 Interception

Interception is a process in which an adversary closely monitors the data being transmitted over the network. The adversaries endeavour to extract the key or relevant information from the data being transmitted. A secure communication framework should be able to resist this attack by ensuring confusion and diffusion among the keys and data so that the attacker can extract minimal or no information related to the keys or the data being transmitted. Both (SOCP & EGCP) the frameworks under discussion ensure confusion and diffusion so an attacker cannot derive any keying information from the data being transmitted over the network between the communicating devices. Neither can any information related to the secure data be extracted based on the Zero Knowledge Proof (ZKP).

4.2.3 DoS Attack

DoS Attack in centralized secure communication schemes refers to the non-availability of a resource to the communication participants. In its severe state the DoS attack can cause the non-availability of the server which results in total hampering of communication. This type of denial can result in delayed key generation

for the entire group or also influence the key management process. SOCP and EGCP are symmetric key protocols that help generate the keys with participant's mutual cooperation and do not fully counter the DoS attack on their own. One thing that is to be brought under consideration is that the DoS attack needs to be countered with the help of host hardening procedures apart from the communication protocols being deployed. Though our frameworks do not ensure 100% security against DoS attack but based on the integration of client registration, participant admission control and authentication to the framework helps thwart the DoS attack to some extent.

4.2.4 Man in the Middle Attack

As the name suggests, man in the middle attack is an attack in which an adversary intercepts the data and tries to gather any information related to the data transmitting over the network or tries to capture the cryptographic keys. This can be termed as a slight variation of the interception process. The only difference is that the adversary isn't monitoring instead becomes part of the communication while not being known to the centralized server or communicating parties. Analysis yields that SOCP and EGCP, both provide high levels of prevention against this attack because the admission control process is in place and the rekeying is being done at regular intervals whenever a session expires or when a participant joins/leaves the communication. Hence the target schemes are capable of circumventing man in the middle attack.

4.2.5 Eavesdropping

Eavesdropping refers to a process in which an adversary listens to the traffic over the network by monitoring the network closely. The aim of the eavesdropper is to capture some of the data being transmitted. The strength of SOCP and EGCP lies in

the fact that all the transmitted data is encrypted with the help of the keys generated directly from the ICMetric basis number prior to transmission. Both the frameworks ensure a high level of confusion and diffusion by using ICMetric number and related mathematical functions. Therefore the eavesdropper can get no advantage of listening to the traffic.

4.2.6 Client-Side Injection Attack

When an attacker sends malicious codes or un-trusted data to the client or participant this type of an attack is termed as the client-side injection attack. The objective of the malicious code is to steal sensitive information such as passwords, cryptographic keys, or data. Hence the client-side injection attack can result in moderate to high level impact on the secure communication. ICMetric technology has the property that the key doesn't need to be stored on the system instead it is generated at run time and discarded after use. Hence even if the attacker initiates an injection attack, the one-to-one or group communication will not be affected by the adversary. Therefore SOCP and EGCP do incorporate countermeasures against client-side injection attack.

Table 4.1 shows an attack metrics narrating the possible attacks on the frameworks (SOCP and EGCP) under discussion. The metric has been populated based on security analysis of the target schemes already performed in this section. The tick (✓) indicates that a scheme has countermeasures incorporated against an attack whereas a cross (×) represents the lack of protection that a scheme provides against a particular attack.

Table 4.1: Attack Metrics for SOCP and EGCP

Attacks	SOCP	EGCP
Brute Force Attack	✓	✓
Interception	✓	✓
DoS Attack	×	×
Man in the middle Attack	✓	✓
Eavesdropping	✓	✓
Client-side Injection Attack	✓	✓

Extensive study [32] shows that in the absence of countermeasures various forms of attacks can have a devastating effect on secure communication. The table 4.2 has been populated after closely analyzing the impact of the possible attacks on the target schemes. The severity of these attacks range from low-moderate-high as shown in the table. If an attack is not possible on a scheme the table mentions the impact of that attack as low.

Table 4.2: Severity of Attacks on SOCP and EGCP

Attacks	SOCP	EGCP
Brute Force Attack	Low	Low
Interception	Low	Low
DoS Attack	Moderate	Moderate
Man in the middle Attack	Low	Low
Eavesdropping	Low	Low
Client-side Injection Attack	Low	Low

From both of these tables it is affirmed that SOCP and EGCP provide a high level of security and are very less prone to attacks.

4.3 Summary

In this chapter we have performed an in depth security analysis of our proposed frameworks, i.e. SOCP and EGCP. Different attacks by the adversary are discussed on both of the protocols by closely analyzing the threats and countermeasures incorporated in our target frameworks. Our analysis yields that the proposed frameworks can provide high end security and can be utilized in highly secure communication applications.

Chapter 5

PERFORMANCE EVALUATION

5.1 Overview

The design and implementation of a scheme/algorithm is incomplete if it is not analysed for its efficiency. In this chapter, the performance of our proposed frameworks (SOCP & EGCP) has been analyzed against similar communication schemes. We have discussed the implementation aspects of our proposed frameworks. The feasibility of our frameworks in a resource constrained environment is discussed. Furthermore based on the Valgrind utility [33], the memory checks and memory consumption has been analyzed.

5.2 Evaluation of Secure One-to-One Communication Protocol

The individual aspects related to the Secure One-to-One Communication Protocol (SOCP) are discussed and evaluated. The entire program is broken down into different modules so that the individual modules can be analyzed effectively. The performance differs from depending upon the system specification where the program is compiled and executed. Therefore before proceeding towards the protocol analysis the system specification and tools need to be discussed

5.2.1 System Tools, Specification and Implementation

The operating system used is Ubuntu 12.04 (Linux Operating System) residing over a virtual machine. The primary resources are 2nd generation core i5, 2.40GHz having 4GB RAM. Whereas the allocated resources to this virtual machine are single processor, 20GB RAM. The Secure One-to-One Communication Protocol has been

implemented in C using the Eclipse platform. The library used is CyaSSL that is an embedded SSL library.

5.2.1.1 CyaSSL Library

CyaSSL embedded SSL library is a crypto-intensive library. It is a lightweight SSL/TLS library written in ANSI C and targeted for embedded, RTOS, and resource-constrained environments - primarily because of its small size, speed, and feature set [33]. This library supports implementation of different ciphers such as AES, DES, SHA etc.

5.2.1.2 Valgrind Profiling

Valgrind is a tool suite that includes profiling and debugging functionality [34]. Valgrind helps perform the following checks:

- Helgrind - It is a thread error detector that helps debug multithreaded programs.
- Cachegrind - It is a cache profiler and helps in cache prediction.
- Memcheck - Helps in memory error detection and identifies accessing memory you shouldn't, unidentified values, incorrect freeing of heap memory, overlapping pointers, memory leaks and overflow.
- Massif - A heap profiler used to perform detailed heap profiling and stack profiling

The SOCP is a single-threaded program hence Helgrind is not used. Our concern is to develop and check the feasibility of our framework in a resource constrained environment for which we want to check the memory consumption and resources used. For this purpose the program has been analyzed by using Valgrind's Memcheck and Massif only.

5.2.2 Secure Remote Password Protocol (SRP)

This is the main module of our framework. The conventional SRP has been extended to perform admission control, key generation and authentication. SRP is basically based on the discrete log problem and SHA-2 for the hashing. The SHA-2 (256) is used in the key generation, authentication and integrity schemes. SHA-256 uses a block size of 512 bits and iterates 64 rounds. Hence all of these schemes are being analyzed collectively in this section. Furthermore we have compared our processing time with the conventional SRP

5.2.2.1 Valgrind based Analysis

Firstly the Valgrind Memcheck is performed on the program. The output asserts that "Valgrind found no problems to report". The next step is to analyze the code using Valgrind Massif profiler. Figure 5.1 shows the Valgrind Massif output. The Massif tool has taken a total of 64 snapshots. The output does not show any error while allocating/deallocating memory to the program. The output does not illustrate any sudden spike either rather the memory is gradually allocated and deallocated. The comparison of the output, snapshots and code indicate the memory usage climbs and falls as expected. Graph shows the heaps and stacks that are allocated to the program.

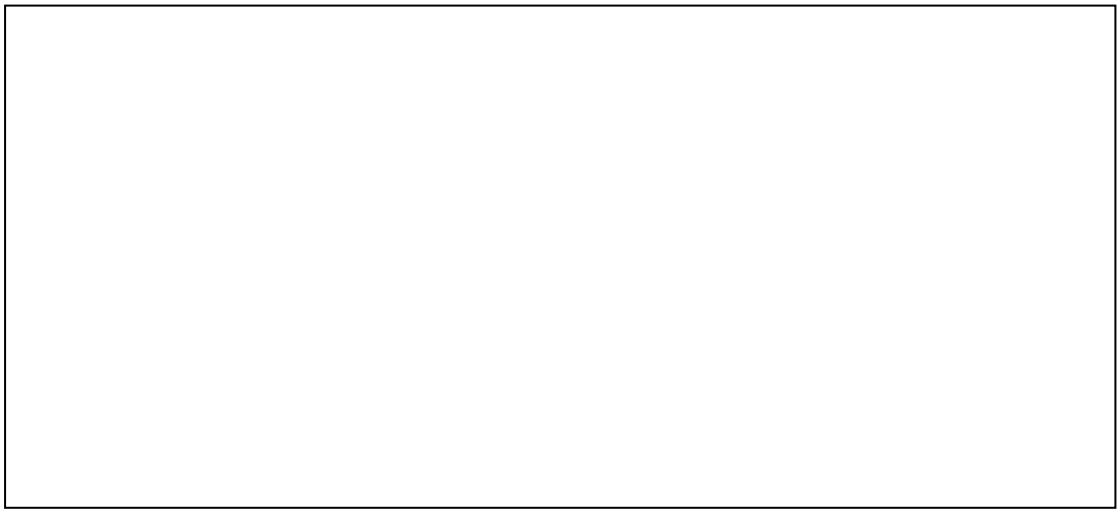

Figure 5.1: Massif Output-Secure Remote Password (SRP) Protocol

5.2.2.2 SRP-CyaSSL vs SRP

We have analyzed our SRP implemented in CyaSSL embedded library for resource constrained environment against the conventional SRP. In [35] the authors have implemented SRP and measured the time program takes to run completely. Their system specification is 700 MHz Pentium III. The program has been implemented in C with the MIRACL and OpenSSL libraries. Figure 5.2 shows the time SRP takes in milliseconds (ms). The computation takes a total of 30.6ms with maximal precomputations.

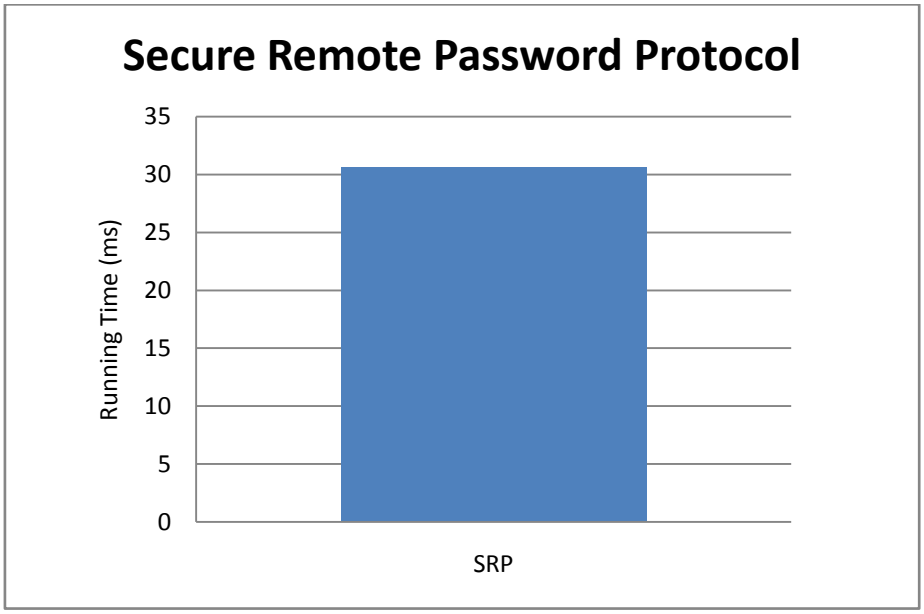

Figure 5.2: Performance Measurement-Secure Remote Password Protocol (SRP)

Our proposed SRP has been implemented and optimized with the help of Valgrind profiling tool. Figure 5.3 shows the time that our program takes in execution. Our SRP protocol takes 5.325ms. Hence our scheme when implemented in C using the CyaSSL Library performs 5.75 times faster. Hence our scheme can be utilized in a resource constrained environment.

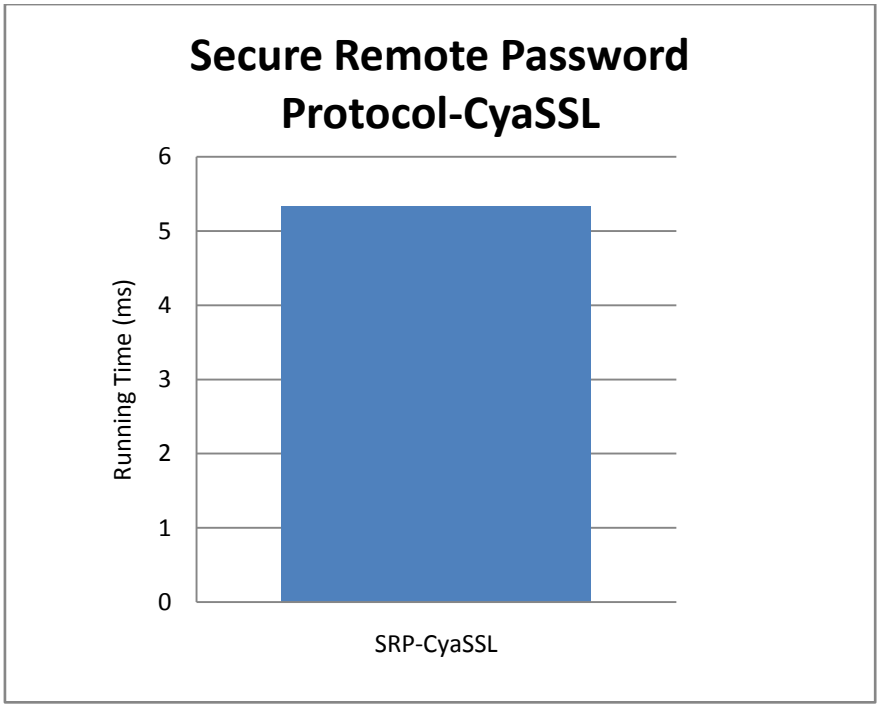

Figure 5.3: Performance Measurement-CyaSSL Secure Remote Password (SRP)

5.2.3 Advanced Encryption Standard (AES)

In SOCP encryption and decryption is very important. It helps hide and protect the data from an adversary during transmission. SOCP uses AES-NI for the encryption/decryption. AES uses 256 bit key and iterates for 14 rounds

5.2.3.1 AES-NI

AES-NI is a CyaSSL library recently developed by Intel [36] solely to be used in a resource constrained environment. It uses new encryption instruction dataset. In [27] the developers of this library have briefly mentioned the six new instructions that help to improve the performance of the conventional AES. Following are the six instructions:

- AESENC & AESENCLAST – AESENC performs single round of encryption and AESENCLAST helps perform the final round of encryption. The functions jointly achieve shift rows, sub bytes and mix columns.

- AESDEC & AESDECLAST – AESDEC performs single round of decryption and AESDECLAST helps perform the final round of decryption. The functions jointly achieve inverse of shift rows, sub bytes and mix columns.
- AESIMC – Converts the round keys into a form that can be used in the inverse ciphers.
- AESKEYGENASSIST – Is used for the generation of the round keys for AES encryption/decryption routines.

5.2.3.2 Valgrind based Analysis

First of all we have performed Valgrind Memcheck on the entire implemented scheme. The output declares that there are no problems to be reported by Valgrind. The next step is to analyze the program using Valgrind Massif profiler. Figure 5.4 shows the Valgrind Massif output. The Massif tool has taken a total of 85 snapshots. The output does not show any error while allocating/deallocating memory to the program. The snapshot analysis doesn't report any error and the memory is gradually allocated and deallocated. The comparative analysis of the output, snapshots and code indicates that the allocated stacks and the memory usage climbs/falls are as expected.

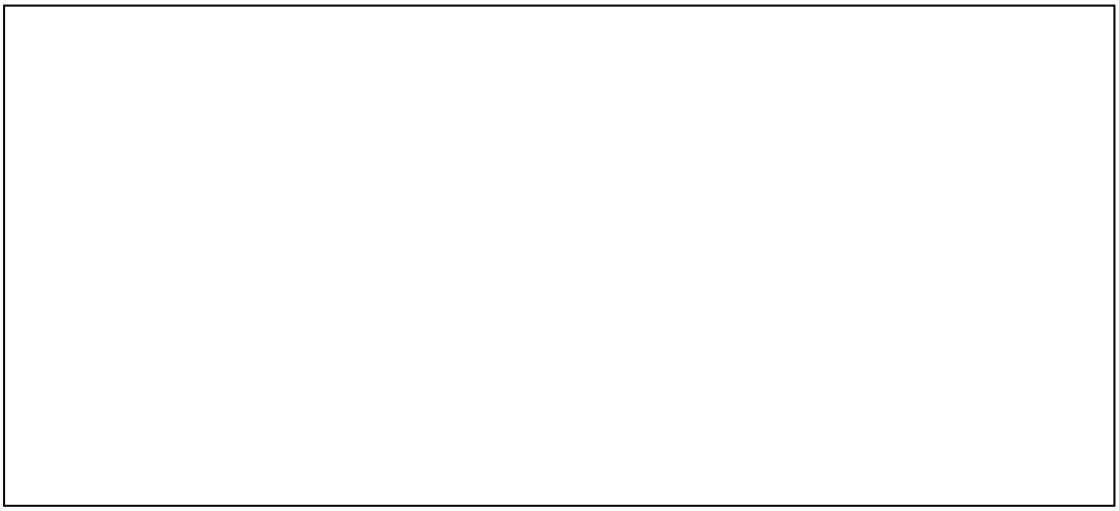

Figure 5.4: Massif Output-AES-NI

5.2.3.3 AES vs AES-NI

In [27] the developers of the AES-NI have already performed a performance analysis of AES-NI versus the standard AES. It is surprising to see that AES-NI is 3.3 times faster as compared to AES. So while consuming less resources AES-NI performs much faster than the traditional software based AES. Figure 5.5 shows the performance of AES-NI versus AES.

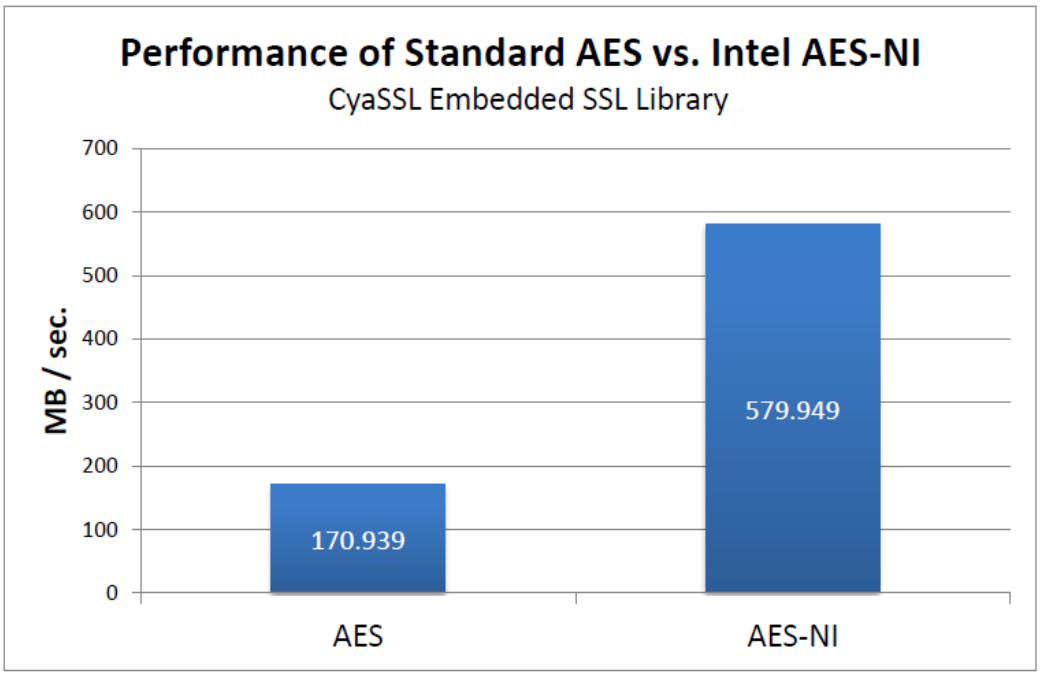

Figure 5.5: Performance Measurement-AES vs AES-NI [27]

5.2.4 Integrity Scheme

The integrity scheme is the most critical requirement of SOCP because it helps authenticate the message. In any embedded system more interest is to correctly identify the modification made to the message while the resource optimization aspect may be compromised a bit. The strength of this scheme lies in the fact that since the same hash function as in the key generation is being used so this scheme can be effective in a resource constrained environment. SOCP framework is designed in such a way that the AES-NI and Integrity scheme coexist. Hence both of the schemes have

been implemented altogether. Therefore the integrity scheme cannot be compared separately with any other similar scheme.

5.2.4.1 Valgrind based Analysis

The analysis starts by firstly performing the Valgrind Memcheck on the program. The output claims that "Valgrind found no problems to report". Therefore this means that there aren't any memory related issues in our program. The next step is to analyze the code using Valgrind Massif profiler. Figure 5.6 shows the Valgrind Massif output. The Massif tool has taken a total of 68 snapshots. The output does not show any error while allocating/deallocating memory to the program. The output does not illustrate any sudden spike either rather the memory is gradually allocated and deallocated. The comparison of the output, snapshots and code indicate the memory usage climbs and falls are as expected. The graph shows the stacks that are being allocated to the program. Our security, performance and complexity analysis yields that this scheme can be deployed in a resource constrained environment.

Figure 5.6: Massif Output-Message Integrity

5.3 Evaluation of Euclidean based Group Communication Protocol

In this section we have performed a critical analysis of the performance of EGCP. Here the only concern isn't measuring the running cost of the framework rather measuring the performance while scaling the number of participants is equally important. The ICMetric basis number has a length of 38 bits and the entropy has been increased to 256 bits.

5.3.1 System Tools, Specification and Implementation

The efficiency and computational analysis is done by implementing the algorithm in C++ and the results are presented in the form of graphs using MAPLE13. The system used is 2nd generation core i5, 2.40GHz having 4GB RAM.

5.3.2 Performance Measurement and Analysis

Three approaches have been adopted to analyze the framework. Firstly the program has been run top down. The next analysis done is for the message generation. Lastly the key generation phase has been analyzed. The data has been interpolated and smoothened with the mechanism of curve fitting. Detailed analysis of EGCP can be found in the proceeding subsections.

5.3.2.1 Top Down Performance Analysis

Firstly we did an analysis of the processing time for the algorithm compiled top down with different group sizes and present the results in the form of graph for analysis. Figure 5.7 shows the running time in milliseconds (ms) along the y-axis versus the group size along the x-axis. We have checked the algorithm by starting with a small group size of 25 members and then increasing the group size additively by 25 members as we move to a maximum of 200 group members. It is evident that

the algorithm assures a linear growth i.e. there isn't any exponential increase for the analyzed data set when the algorithm is fully run.

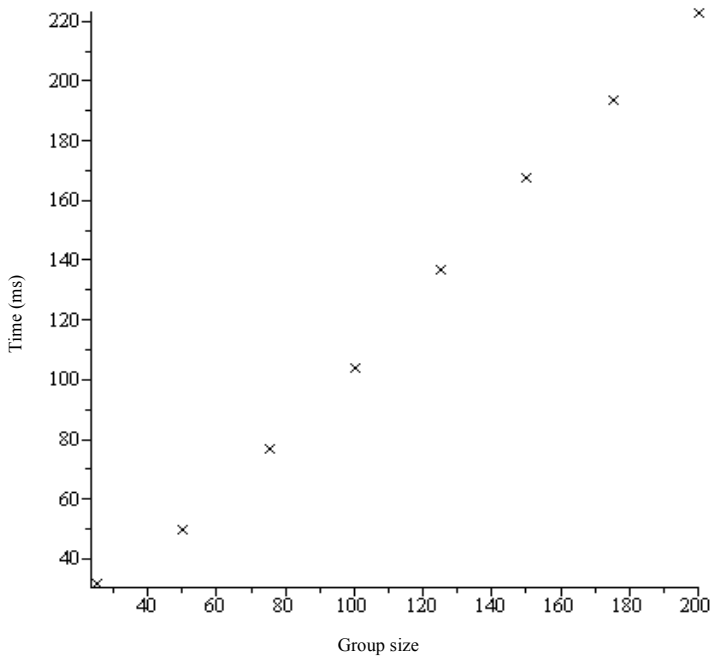

Figure 5.7: Running Time (ms) for the algorithm to run top down

5.3.2.2 Message Generation Cost Analysis

Message generation is a very important aspect of EGCP because the key generation is directly dependent on it. Figure 5.8 shows a graphical representation of the running time in milliseconds (ms) of the algorithm for the message generation and transmission. As discussed in chapter 3, it is the task of the key distribution manager also termed as the GC to generate the message and transmit it to the client in order to further generate the group key. The computation has been scaled to 200 participants and it can be observed that the running time linearly relates to the number of participants who are taking part in the group communication.

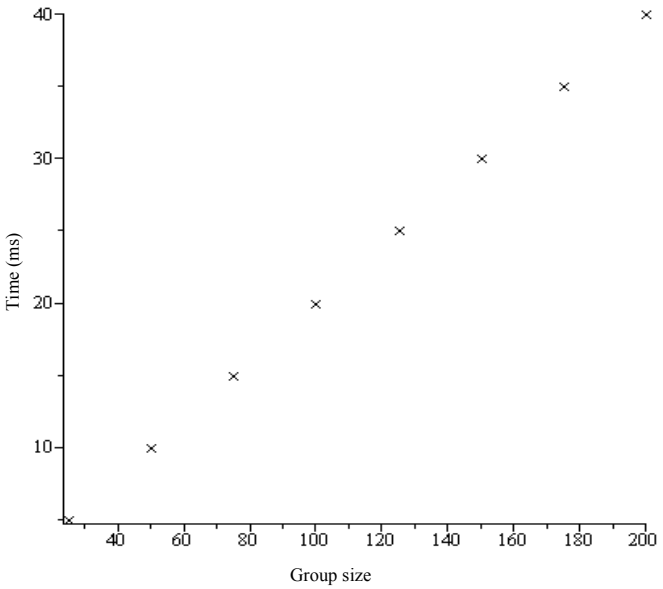

Figure 5.8: Running Time (ms) for Message Generation

5.3.2.3 Key Generation Cost Analysis

Figure 5.9 shows the running time of the system to generate keys for the corresponding messages that were generated by the GC and transmitted to the client. This is entirely based on the computation of Euclidean Algorithm as explained previously and is carried out on the client's system. It can be seen that again this graph is also linear. The key generation was also checked up to a total of 200 participants.

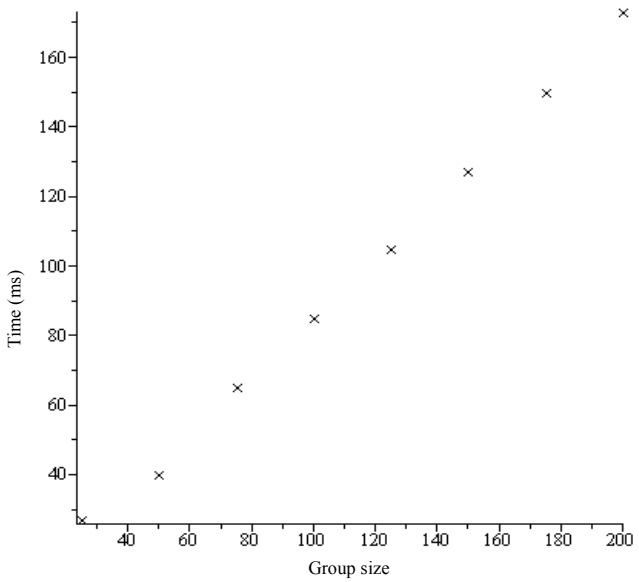

Figure 5.9: Running Time (ms) for Key Generation

Keeping all of the running time plotted against the group size under consideration it is evident that all the phases of the algorithm take reasonable time to compute the messages and the keys. Even if tested on a total of 200 participants the threshold isn't approached. That is till 200 participants there isn't any sudden increase in the time consumption. Hence this algorithm can definitely be used for large datasets and in settings that require a large number of participants to communicate not only securely but also efficiently. This framework can be used in a resource constrained environment.

5.3.3 Comparative Analysis

This section performs a comparative performance analysis of EGCP among another renowned scheme that can be used in secure group communication i.e. One-Way Function key Tree (OFT). The tree based scheme requires a centralized server to generate and compute the cryptographic keys whereas EGCP generates the keys at run time. Both of these schemes provide key generation and key management but the characteristic common to these schemes is that they are centralized by design. Furthermore, the keys generated by the schemes are symmetric.

5.3.3.1 One-way Function Key Tree

One-Way Function Key Tree (OFT) [37][38] is a tree based scheme that uses one-way hash functions to generate symmetric keys. This scheme reduces the load on the group controller as some computations are performed by the participants involved in the communication. The OFT key management scheme is based on the one-way hash function $h(\ )$ and a mixing function $f(a, b)$. Details of this scheme are as under:

5.3.3.1.1 *One-way Function* $h(\,)$

The keys are passed through a strong one-way hash function that serves to hide the contents of the original key. Since the keys (known as blinded keys) are hashed therefore they can be shared without any concern. The properties of hashing ensure that the blinded keys cannot be reversed to reveal the true keys.

5.3.3.1.2 *Joining Function* $f(a, b)$

This function concatenates or combines the participant's hashed keys. Any participant can compute the key by using the following formula

$$k_i = f\left(h\left(k_{left\,(i)}\right), h\left(k_{right_{(i)}}\right)\right)$$

Where $k_{left\,(i)}$ and $k_{right_{(i)}}$ denote left and right children node of the parent node respectively. Figure 5.10 shows a generalized OFT.

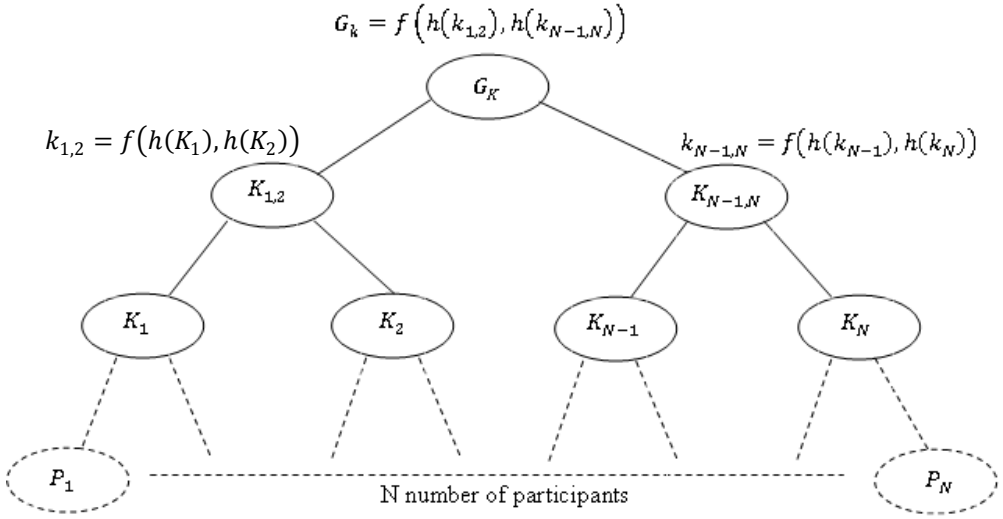

Figure 5.10: One-way Function Key Tree (OFT)

Since every participant knows its own hashed key and the hashed key of the sibling therefore the participant can easily compute the respective session keys with the help of the joining function $f(a, b)$. The group controller uses the keys of the participants to compute the group key based on $f(a, b)$. So it can be seen that in

thekey generation mechanism, sole responsibility does not rely on the group controller. Rather most of the tasks are being performed by the participants. The group controller calculates each key of the parent node/ root node and sends it back to the participants by encrypting it with their respective keys.

5.3.3.2 Comparative Performance Measurement

EGCP has been analyzed against the OFT scheme. The underlying Hash function used in OFT is SHA-2. Our analysis will be based on two aspects; firstly the running time when the schemes are run top down i.e. from the start till the end. Our second analysis will be based on studying the running for the key generation and key distribution process. The graphs are generated with the help of Maple 13 [39] and they depict the cost in terms of time and total number of participants.

Figure 5.11 graphically shows the running time for both the schemes when run top down. Both schemes have been analyzed by comparing number of participants and the time in milliseconds (ms). Y-axis shows the running time of the schemes whereas X-axis represents the total number of participants in the group. The group communication starts with a relatively small group size of 25 participants and then gradually 25 participants are added until a total of 200 participants is reached. It can be seen that the OFT scheme (cross plot) shows a linear growth as the number of participants reach 200. Whereas EGCP (circle plot) performs better by consuming less running time which is also evident from the linear growth of the graph. The points have been interpolated and the data has been smoothed through curve fitting.

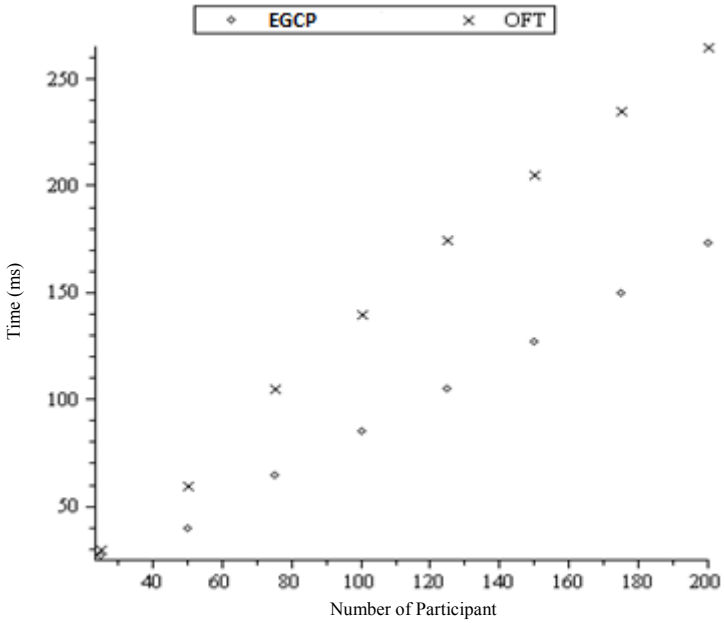

Figure 5.11: Running Time (ms)-Top down for EGCP vs OFT

It is necessary to analyse the scheme from a key generation perspective. This is one of the most important and time consuming task in any secure communication protocol. Figure 5.12 gives comparative analysis by graphically representing the running time that the schemes take for the key generation and key distribution among the participants. Again the same process has been followed as for the generation of the graph above and the system specification remain the same. Again both schemes have been analyzed by scaling them from 25 to 200 participants. As shown previously the group again comprises of 25 participants in the beginning and is incremented by 25 participants gradually until the group size reaches to 200. The time is measured in milliseconds (ms) and is along the Y-axis. It can be seen that the EGCP (circle plot) requires less time as compared to the OFT (cross plot). OFT shows an exponential growth whereas EGCP shows a linear growth. Hence EGCP scheme possesses better scalability properties in the key generation phase, as the OFT scheme consumes more time.

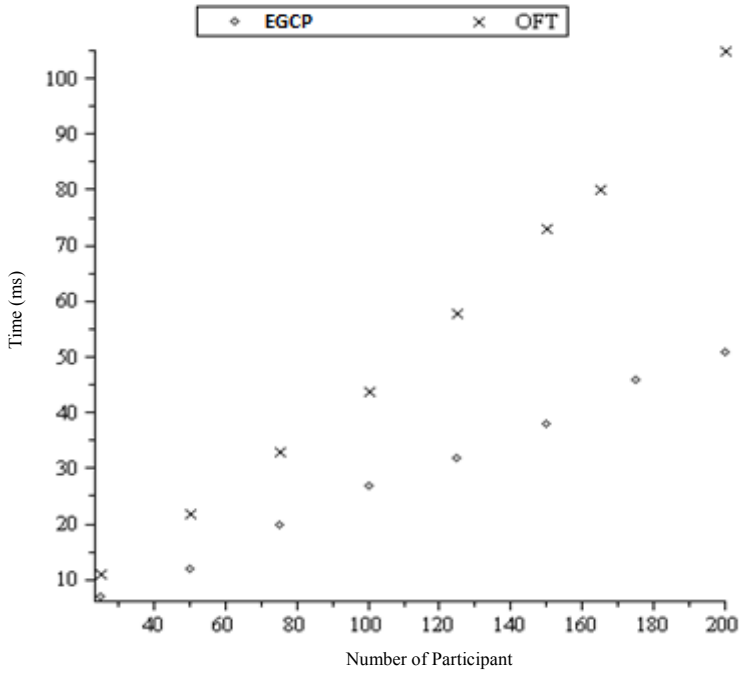

Figure 5.12: Running Time (ms)-Key Generation for EGCP vs OFT

The analysis yields that in terms of cost, EGCP has performed better as compared to the contending scheme. OFT has a greater overhead and requires more resources as compared to EGCP. Therefore in a resource constrained environment EGCP can give the optimal results along with better security provisions.

5.4 Summary

In this chapter the proposed frameworks have been analyzed by measuring their performance. The schemes have been implemented and the time has been measured. SOCP has been analyzed using Valgrind profiler that helps in performing memory check. The memory allocation and deallocation has been administered with the help of Valgrind Massif. EGCP has been analyzed for the time while gradually scaling the number of participants to 200. The aim is to check whether the threshold is approached on joining 200 participants to the network. The results of both of the frameworks yields that they can be deployed in a resource constrained environment without giving a second thought.

Chapter 6

CONCLUSION AND FUTURE WORK

6.1 Overview

In this era secure communication is a thought provoking task because with the advancement made in the field of Information Security the attackers are becoming more intelligent and sophisticated. The probable attacks can be narrowed down by incorporating the ICMetric technology in the existing systems. Though ICMetric technology is a new concept in the field of IT but it has brought revolution to the designing of secure communication protocols. This research focuses on the use of ICMetric technology in the designing of secure communication frameworks.

This chapter gives a brief overview of the work done and goals achieved through this research. Towards the end the Future work in the field of ICMetric has been proposed and the research has been concluded.

6.2 Overview of Research

When it comes to secure communication the one-to-one communication and group communication both need to be dealt with accordingly and separately. Current cryptographic communication schemes and protocols are heavily reliant on stored keys. If these keys are captured/ exposed then the system can be easily penetrated. To counter this fundamental yet common problem the latest ICMetric technology has been designed. Our research focuses towards the development of state of the art cryptographic frameworks that facilitate the secure communication.

Our contributions in this area of research has helped in developing attack resilient systems. Perhaps the greatest advantage of this technology is that it is being

designed so that it interoperates with existing technologies. The ICMetric technology adds another security layer onto the existing security systems.

6.3 Achievements

In this research, we have proposed two new comprehensive symmetric cryptographic protocols for secure communication. SOCP is a protocol designed to facilitate the communication between two parties whereas EGCP is designed to facilitate the multiparty communication. Both of the proposed frameworks are based on the utilization of the ICMetric Technology. The ICMetric based symmetric cryptographic protocols provide fundamental security features like authentication, confidentiality and integrity of data. The designed frameworks provide high level of security based on comprehensive modules without compromise on resource constraints. This research can have much impact on security systems. We ultimately performed a security analysis and thus heuristically argued that the protocols obtain the desired security attributes. We have compared the protocol's efficiency to available authentication and encryption/ decryption solutions. Towards the end the computational costs of the target schemes have been computed by interpolating the data and smoothening it with the mechanism of curve fitting.

6.4 Future Work

This thesis primarily focuses on the utilization of the ICMetric technology in secure communication. What is to be understood is that even the best schemes cannot offer fool proof security. One of the most difficult tasks in the field of digital forensics is the identification of a theft and the motives behind an incident. As discussed earlier that ICMetric basis number changes if the hardware or software environment changes. Though the system tempering in the ICMetric technology can be detected easily yet

the use of ICMetric technology in the field of digital forensic is still to be explored. From an initial analysis it is very clear that the ICMetric technology can assist forensic investigators because the ICMetric basis number is in fact a digital fingerprint of a system. Consequent to the wide scale adoption of the ICMetric technology it can be said that this technology can help forensic investigators in effective and efficient digital inquiries.

Furthermore experiments focusing on the incorporation of the ICMetric technology in other systems are already underway. The technology is being studied by implementing it on a cryptographically secure battery powered wheelchair [23]. The ICMetric technology uses the human machine interface, navigation data and dynamic controls for the generation of system identification. Other systems upon which research is underway include autonomous systems, driverless vehicles, single and group communications.

Currently everything around us uses digital circuitry based on high speed processors, memories, hard drives, sensors etc. A recent but fairly popular area of research is Internet of Things (IoT). Using this technology different embedded computing devices, internet enabled household devices, vehicles, televisions, etc can be interconnected with each other via the existing internet infrastructure. Hence the ICMetric of Things (ICMoT) is a revolutionary new concept that can be used to secure IoT. With the help of ICMetric technology we can identify every device over the existing infrastructure uniquely.

6.5 Conclusion

Traditionally the Achilles heel in cryptography has been the theft of keys. No matter which cryptographic technique is utilized it stands no chance if the keys are

compromised. Therefore effort is needed to secure cryptographic keys. Based on our research and detailed analysis of ICMetric based secure communication symmetric scheme can be termed as a breakthrough in the field of information security. Furthermore the ICMetric technology coupled with our secure communication frameworks (SOCP, EGCP) possesses the potential to defeat a wide range of attacks which are commonly seen successful on modern systems. Here it can confidently be concluded that the ICMetric technology can offer the highest levels of security at the cost of little or no additional resources.

BIBLIOGRAPHY

[1] E. Gilmer, "Privacy and Security of Patient Data in the Cloud," IBM Corporation, 2013.

[2] H. Tahir, G. Howells, H. Hu, D. Gu, and K. McDonald-Maier, "On the incorporation of secure filter in ICMetrics group communications," in *Fifth International Conference on Emerging Security Technologies*, 2014, pp. 1-5.

[3] A. Hopkins, K. McDonald-Maier, and G. Howells, "Patent Identifier No. WO 2008015421 A1," University of Essex Enterprises Limited, 2013.

[4] Y. Kovalchuk, et al., "Investigation of properties of ICMetric features," in *Third International Conference on Emerging Security Technologies*, 2012, pp. 115-120.

[5] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions of Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[6] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication," in *3rd ACM Conference on Computer and Communications Security*, 1996, pp. 31-37.

[7] A. Yasinsac, V. Thakur, S. Carter, and I. Cubukcu, "A family of protocols for group key generation in adhoc networks," in *International Conference on Communications and Computer Networks*, 2002, pp. 183-187.

[8] E. Bresson, O. Chevassut, and D. Pointcheval, "Provably authenticated group Diffie-Hellman key exchange-the dynamic case," *Springer Lecture Notes in Computer Science*, vol. 2248, pp. 290-309, 2001.

[9] H. Krawczyk, *HMQV: A High-Performance Secure Diffie-Hellman Protocol*. Springer, 2005, vol. 3621.

[10] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones, "Group-based secure communication for large-scale wireless sensor networks," *Journal of Information Assurance and Security*, pp. 139-149, 2007.

[11] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 60-96, 2004.

[12] M. Howarth, S. Iyengar, Z. Sun, and H. Cruickshank, "Dynamics of key management in secure satellite multicast," *IEEE Journal on Selected Areas in Communication*, vol. 22, no. 2, pp. 308-319, 2004.

[13] B. Lai, S. Kim, and I. Verbauwhede, "Scalable session key construction protocol for wireless sensor networks," in *IEEE Workshop on Large Scale Real Time and Embedded Systems*, 2002, p. 7.

[14] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in adhoc networks: a probabilistic approach," in *11th IEEE International Conference on Network Protocols*, 2003, pp. 326-335.

[15] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: challenges and opportunities ," in *arXiv preprint*, 2015.

[16] A. C. Davies, "WW2 british army battlefield wireless communications equipment.," in *In History of Telecommunications Conference* , 2008, pp. 83-90.

[17] X. Zhai, et al., "Application of ICMetrics for embedded system security," in *Fourth International Conference on Emerging Security Technologies*, 2013, pp. 89-92.

[18] E. Papoutsis, "Investigation of the potential of generating encryption keys for ICMetrics," Kent University, 2009.

[19] E. Papoutsis, G. Howells, A. Hopkins, and K. McDonald-Maier, "Integrating

feature values for key generation in an ICMetric system," in *NASA/ESA Conference on Adaptive Hardware and Systems*, 2009, pp. 82-88.

[20] Y. Kovalchuk, H. Hu, D. Gu, and K. McDonald-Maier, "ICmetrics for low resource embedded systems," in *Third International Conference on Emerging Security Technologies*, 2012, pp. 121-126.

[21] R. Tahir, H. Hu, D. Gu, G. Howells, and K. McDonald-Maier, "A scheme for the generation of strong ICMetrics based session key pairs for secure embedded system application," in *The 27th IEEE Interational Conference on Advanced Information Networking and Applications*, Barcelona, Spain, 2013.

[22] Y. Kovalchuk, K. McDonald-Maier, and G. Howells, "Overview of ICMetrics technology-Security infrastructure for autonomous and intelligent healthcare system," *International Journal of u- and e- Service, Science and Technology*, vol. 4, no. 3, pp. 49-60, 2011.

[23] A. Kokosy, et al., "SYSIASS – an intelligent powered wheelchair," in *1st International Conference on Systems and Computer Science*, Lille, 2012.

[24] H. Tahir, R. Tahir, and K. McDonald-Maier, "A Novel Private Cloud Document Archival System Architecture Based on ICmetrics," in *Fourth International Conference on Emerging Security Technologies (EST)*, 2013, pp. 102-106.

[25] Y. Bin, G. Howells, and M. Haciosman, "Investigation of Properties of ICmetric in Cloud," in *Fourth International Conference on Emerging Security Technologies (EST)*, 2013, pp. 107-108.

[26] M. Rahman and W. M. Cheung, "Cloud computing, security issues and potential solution by using ICMetrics or Biometrics based encryption," in *International Conference on Advances in Computing, Electronics and Communication*, 2013,

pp. 36-41.

[27] R. Tahir, *Communication frameworks based on ICMetric*. Unpublished.

[28] R. Chesebrough and C. Conlon, "Implementation and Performance of AES-NI in CyaSSL Embedded SSL," Intel & yaSSL, 2012.

[29] M. Venkatesulu and K. Kartheeban, "EAB-Euclidean Algorithm based key communication protocol for secure group communication in dynamic grid environment," *International Journal of Grid and Distributed Computing*, vol. 3, no. 4, pp. 45-55, 2010.

[30] G. J. Woeginger, "Exact algorithms for NP-hard problems: A survey," *Combinatorial Optimization—Eureka, You Shrink!*, pp. 185-207, 2003.

[31] A. Almulhem, "Threat modeling for electronic health record systems," *Journal of medical systems*, vol. 36, no. 5, pp. 2921-2926, 2012.

[32] R. Tahir, H. Hu, D. Gu, McDonald-Maier, and G. Howells, "Resilience against brute force and rainbow table attacks using strong ICMetrics session key pairs," in *1st International Conference on Communications, Signal Processing, and their Applications* , 2013, pp. 1-6.

[33] M. M. Noor and W. H. Hassan, "Wireless networks: developments, threats and countermeasures," *International Journal of Digital Information and Wireless Communications*, vol. 3, no. 1, pp. 119-134, 2013.

[34] Valgrind, "Valgrind Documentation," Manual 3.10.0, 2014.

[35] wolfSSL. (2015) WolfSSL website. [Online]. http://wolfssl.com/yaSSL/Products-cyassl.html

[36] P. Hamalainen, M. Hannikainen, M. Niemi, and T. Hamalainen, "Performance evaluation of Secure Remote Password protocol," in *International Symposium on*

Circuits and Systems, vol. 3, 2002.

[37] Intel Corporation. (2010) Intel Data Protection Technology with AES-NI and Secure Key. [Online]. http://www.intel.com/

[38] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Transactions on Software Engineering*, vol. 29, no. 5, pp. 444-458, 2003.

[39] W. C. Ku and S. M. Chen, "An improved key management scheme for large dynamic groups using one-way function trees," in *IEEE International Conference on Parallel Processing Workshops*, 2003, pp. 391-396.

[40] J. L. G. Pardo, *Introduction to cryptography with maple*. Springer-Verlag Berlin Heidelberg, 2013.

RELATED RESEARCH PUBLICATIONS

Conference Papers:

S. Tahir, I. Rashid, "A Key Management Scheme for Secure Communication Based on ICMetric", accepted and to appear in proceedings of IEEE Science and Information Conference 2015, London, 28-30 July, 2015.

S. Tahir, M. Afzal, M. Tahir, "An ICMetric based Key Generation Scheme for Controlled Group Communication", The Fifth IEEE International Conference on Information, Intelligence, Systems and Applications (IISA 2014), Chania Crete**,** Greece, pp. 373-378, 7-9 July, 2014.

Book Chapter:

Chapter Proposal titled "ICMetric Based Secure Communication" accepted for Handbook of Research on Innovations in Access Control and Management, for release in the Advances in Information Security, Privacy and Ethics (AISPE) Book Series, IGI Global. The full chapter will be submitted before 15th March, 2015.