Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 16 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

RASCP: Providing for a Secure Group Communication Plane Using RFID

By K S Jagadeesh, Dr. Somashekhar C Desai, Chandramouli.H & Kashyap D Dhruve

JJT University, Jhunjhunu, Rajasthan, India

Abstract - Predominantly large distributed networks currently provide support for group oriented protocols and applications. Regardless of the type of distributed network there is a need to provide communication privacy and data integrity to the information exchange amongst the group members. This paper introduces a protocol named *RFID* Authentication based Secure Communication Plane *(RASCP)*. *RASCP* adopts the commutative RSA algorithm to maintain data integrity. The proposed protocol not only eliminates the overheads resulting from key distribution and key compromise attacks but also provide for information security in the presence of colluded group members. Radio Frequency Identification *(RFID)* tags is used for group member identification. The RACP protocol is compared with the RFID extended Secure Lock *(RSL)* group communication protocol and its efficiency in terms of the computational complexity involved is discussed in this paper.

Keywords : RFID, RFID security, RFID authentication secure group communication, cryptography, commutative rsa, secure plane, computational cost, sieve of eratosthenes algorithm , prime numbers, pseudo random number generators, secure lock.

GJCST-E Classification : E.3

RASCP PROVIDING FOR A SECURE GROUP COMMUNICATION PLANE USING RFID

Strictly as per the compliance and regulations of:

RASCP: Providing for a Secure Group Communication Plane Using RFID

K S Jagadeesh [α], Dr. Somashekhar C Desai [σ], Chandramouli.H [ρ] & Kashyap D Dhruve [Ѡ]

Abstract - Predominantly large distributed networks currently provide support for group oriented protocols and applications. Regardless of the type of distributed network there is a need to provide communication privacy and data integrity to the information exchange amongst the group members. This paper introduces a protocol named $\boldsymbol{RFID}$ Authentication based Secure Communication Plane $(\boldsymbol{RASCP})$. $\boldsymbol{RASCP}$ adopts the commutative RSA algorithm to maintain data integrity. The proposed protocol not only eliminates the overheads resulting from key distribution and key compromise attacks but also provide for information security in the presence of colluded group members. Radio Frequency Identification $(\boldsymbol{RFID})$ tags is used for group member identification. The RACP protocol is compared with the RFID extended Secure Lock $(\boldsymbol{RSL})$ group communication protocol and its efficiency in terms of the computational complexity involved is discussed in this paper.

Keywords : RFID, RFID security, RFID authentication secure group communication, cryptography, commutative rsa, secure plane, computational cost, sieve of eratosthenes algorithm , prime numbers, pseudo random number generators, secure lock.

I. Introduction

RFID systems and standards established by IEEE [1,2] are envisioned to be one of the most commonly used identification mechanisms in the near future [3]. A RFID authentication system primarily consists of a tag and a reader with a database to store the tag details. Tags available are of several types and classes [1][2] but the research work presented here considers the most commonly available passive RFID tags of class 0. A lot of research is ongoing to provide security to the existing standards and the technology involved in manufacturing and Radio Frequency (RF) communication systems in place. Currently there exist several threats to the existing RFID deployments like Denial of Service Attacks, RFID Tag Cloning, RFID Tag Tracing, Eavesdropping, Replay Attacks Data Forging, Invading Privacy Information and Hot-listing to name a few [3][4][5][6][7][8][9][10]. More often than not researchers have focused on the eliminating the threats that currently exist in the RFID technology and methods towards improving it. In the research work presented here the use of the existing RFID technology for identification is adopted. The proposed protocol i.e. $RASCP$ assumes that the RFID communication module considered is secure and free of the above mentioned defects/attacks.

Communication provisioning is considered as the basic essentials of any network. The prevalent large scale distributed networks existent provide support for various business, personal, commerce, banking, military, intelligence applications and services. These networks are prone to varied kind of attacks and data compromise issues. To counter the issue of data compromise cryptography is commonly used. Cryptographic algorithms could be broadly classified into two types namely Symmetric and Asymmetric type. The $RASCP$ protocol proposed utilizes the asymmetric commutative RSA Algorithm to provide for security. These algorithms are discussed in detail in the future sections of this paper.

The remaining paper is organized as follows. Section II discusses the commutative RSA algorithm. The Sieve of Eratosthenes prime number generation algorithm is discussed in the next section. The fourth section of the paper provides an in depth explanation of the proposed $RASCP$group communication scheme. The fifth section of the paper presents the RFID extended secure lock group communication scheme. The penultimate section of the paper discusses the experimental evaluation wherein the propose $RASCP$ and the RSL are compared. The conclusion and the future work is discussed in the last section of the paper.

II. Commutative Rsa

A secure plane is realizable provided the data communicated over the plane is protected and cannot be colluded. The use of cryptographic techniques is generally preferred, hence the $RASCP$ proposed in this paper adopts the commutative RSA algorithm. The $RASCP$ considers two prime numbers $Param\_P_p^{CRSA}$ and $Param\_Q_q^{CRSA}$ initialized amongst all the group members. Let G_A and G_B represent the group members required to communicate over the secure plane. To compute the encryption keys and decryption key pairs of the commutative RSA algorithm the parameters

Author α : Research Scholar, JJT University, Jhunjhunu, Rajasthan, India. E-Mail : Ksj_20012002@yahoo.co.in
Author σ : Professor, BLDEA College of Engineering, Bijapur, India. E-Mail : desaisc07@gmail.com
Author ρ : Research Scholar, JJT University, Jhunjhunu, Rajasthan, India. E-Mail : hcm123cool@rediffmail.com
Author Ѡ : Technical Director, Planet-I Technologies, Bangalore, India. E-Mail : kashyapdhruve@hotmail.com

$Param\_N^{CRSA}$ and $Param\_\phi^{CRSA}$ are computed using the following

$$Param\_N^{CRSA} = [(Param\_P_p^{CRSA}) \times (Param\_Q_q^{CRSA})]$$

$$Param\_\phi^{CRSA} = [(Param\_P_p^{CRSA} - 1) \times (Param\_Q_q^{CRSA} - 1)]$$

From the above equations it is clear that $Param\_N_A{}^{CRSA} = Param\_N_B{}^{CRSA}$ and $Param\_\phi_A{}^{CRSA} = Param\_\phi_B{}^{CRSA}$ for A and B. The encryption key pair of A and B represented as

$(Param\_N_A{}^{CRSA}, Param\_E_A{}^{CRSA})$ and

$(Param\_N_B{}^{CRSA}, Param\_E_B{}^{CRSA})$

is to be obtained. The $Param\_E^{CRSA}$ is obtained by randomly selecting numbers such that it is a co prime of $Param\_\phi^{CRSA}$ or in other terms

$$\mathcal{Fn}_{GCD}(Param\_E^{CRSA}, Param\_\phi^{CRSA}) = 1$$

Where $\mathcal{Fn}_{GCD}(x,y)$ represents the greatest common divisor function between two variables x and y.

The decryption key pair of A and B is represented by $(Param\_N_A{}^{CRSA}, Param\_D_A{}^{CRSA})$ and $(Param\_N_B{}^{CRSA}, Param\_D_B{}^{CRSA})$ and the parameter $Param\_D^{CRSA}$ is computed based on the following equation

$$Param\_D^{CRSA} = (Param\_E^{CRSA})^{-1}\ Mod(Param\_N^{CRSA})$$

Let Enc_X represent the encrypted data X. The encryption operation is defined as follows

$$Enc_X = X^{Param\_E^{CRSA}}\ Mod(Param\_N^{CRSA})$$

The commutative RSA decryption operation on the encrypted data Y is defined

$$Dec_Y = Y^{Param\_D^{CRSA}}\ Mod(Param\_N^{CRSA})$$

a) Commutative proof RSA Algorithm

The commutative property of the RSA algorithm adopted in $RASCP$ can be proved if data X encrypted by A and then encrypted by B provides the same resultant if the encryption is performed by B followed by the encryption performed by A i.e.

$$Enc^B(Enc_X{}^A) \equiv Enc^A(Enc_X{}^B)$$

$$Enc^B\left(X^{Param\_E_A{}^{CRSA}}\ Mod(Param\_N_A{}^{CRSA})\right) \equiv Enc^A\left(X^{Param\_E_B{}^{CRSA}}\ Mod(Param\_N_B{}^{CRSA})\right)$$

$$X^{(Param\_E_A{}^{CRSA} \times Param\_E_B{}^{CRSA})}\ Mod(Param_{N_A}{}^{CRSA}) = X^{(Param\_E_B{}^{CRSA} \times Param\_E_A{}^{CRSA})}\ Mod(Param\_N_B{}^{CRSA})$$

As $Param_{N_A}{}^{CRSA} = Param\_N_B{}^{CRSA}$ it can be concluded that

$$X^{(Param\_E_A{}^{CRSA} \times Param\_E_B{}^{CRSA})}\ Mod(Param_{N_A}{}^{CRSA}) = X^{(Param\_E_B{}^{CRSA} \times Param\_E_A{}^{CRSA})}\ Mod(Param\_N_A{}^{CRSA})$$

And hence

$$Enc^B(Enc_X{}^A) \equiv Enc^A(Enc_X{}^B)$$

III. Prime Number Generation

Prime number generation functions and their application to the arena of cryptography have been extensively studied by researchers. The $RACP$ proposed in this paper utilizes the Sieve of Eratosthenes Algorithm [11] to find a set of prime numbers based on the user $RFID$ tags. Let n_{Max} represent a number derived from the user $RFID$ tag. Let us consider a Boolean Set B_{Tmp} having n_{Max} Boolean values, each element are represented as b_{Indx} where $b \in \{T, F\}$ and $Indx$ represents the index corresponding to the number in $\mathcal{N}_{Tmp} = \{2,3,4, \dots \dots n_{Max}\}$. Let $Var1 = F_{Least}(n, \mathcal{N}_{Tmp}, B_{Tmp})$ represent a function that returns the smallest number $Var1 \in \mathcal{N}_{Tmp}$ in $\mathcal{N}_{Tmp}$ that is greater than n and $b_n = F$ and $b_n \in B_{Tmp}$. The Sieve of Eratosthenes Prime number generation algorithm is adopted to generate prime number set P. The Sieve of Eratosthenes algorithm adopted is given below

Algorithm 1: Sieve of Eratosthenes Prime number generation algorithm

Input:

User RFID based Number $\boldsymbol{n_{Max}}$

Output:

Prime Number Set $\boldsymbol{P}$

Algorithm:

I. Initialize $\mathcal{N}_{Tmp} = \{2,3,4, \dots \dots n_{Max}\}$
II. Initialize Boolean set $B_{Tmp} = \{F_1, F_2, F_3, \dots \dots F_{n_{Max}}\}$
III. Initialize $Var = 2$
IV. Do
V. Set the index of all the multiples of $Var1$ to True i.e. T occurring between Var^2 and n_{Max}.
VI. $Var = F_{Least}(Var, \mathcal{N}_{Tmp}, B_{Tmp})$
VII. While $(Var^2 > n_{Max})$
VIII. P = Set of all indexes of $b_{Indx} \in B_{Tmp} : b_{Indx} = F$

From the above algorithm it is evident that the set P obtained contains all the prime numbers between 2 and n_{Max}. This algorithm is utilized to obtain the probable $P_{Comm\_RSA}^{Prob}$ and $Q_{Comm\_RSA}^{Prob}$ sets required to initialize the commutative RSA algorithm in the $RACP$ for each user considered in the communication plane. The computational complexity of this algorithm is $O(n_{Max} \ln \ln n_{Max})$[12][13].

IV. RASCP - RFID Authentication Based Secure Communication Plane

Let us consider a set of users who would like to communicate securely represented by a set defined as

$G = \{g_1, g_2, g_3, \dots \dots g_m\}$

Where g_m represents the m^{th} user of the group G.

It is assumed that each user $g_m \in G$ posses a RFID Tag represented as T^m and an RFID reader. The RFID tags are said to contain data of length L_T^m where m represents the m^{th} user and the users associated tag T^m. The secure communication plane is constructed by adopting the commutative RSA algorithm. To initialization of the commutative RSA algorithm is based on the RFID tag data $RFID_T^m$, used to obtain the parameters $Param\_P_m^{CRSA}$ and $Param\_Q_m^{CRSA}$ using the Sieve of Eratosthenes Prime number generation algorithm. Each member of the group contributes towards the construction of the commutative RSA sets $PARAM\_P$ and $PARAM\_Q$ defined as

$PARAM\_P = \{Param\_P_1^{CRSA}, Param\_P_2^{CRSA}, \cdots, Param\_P_m^{CRSA}\}$ and

$PARAM\_Q = \{Param\_Q_1^{CRSA}, Param\_Q_2^{CRSA}, \cdots, Param\_Q_m^{CRSA}\}$

The algorithm used to construct the $PARAM\_P$ and $PARAM\_Q$ sets is as mentioned below

Algorithm Name: $PARAM\_P$ and $PARAM\_Q$ construction

Input:

I. Group Member Set $\boldsymbol{G} = \{\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3}, \dots \dots \boldsymbol{g_m}\}$

II. Group RFID Tag Associated with each Group Member $\boldsymbol{g_m}, \boldsymbol{T^m}$ and its data $\boldsymbol{RFID_T^m}$ and length $\boldsymbol{L_T^m}$

Output:

I. $\boldsymbol{PARAM\_P}$

II. $\boldsymbol{PARAM\_Q}$

Algorithm

I. Initilize $PARAM\_P = \emptyset$ and $PARAM\_Q = \emptyset$

II. For Each group member $g_m \in G$

III. $\vec{Q}_{Tmp}^m, \vec{P}_{Tmp}^m = Split(L_T^m, RFID_T^m)$

IV. $P_{Comm\_RSA}^{Prob\ m} = GetPrimeSet(\vec{P}_{Tmp}^m)$

V. $Q_{Comm\_RSA}^{Prob\ m} = GetPrimeSet(\vec{Q}_{Tmp}^m)$

VI. $Param\_P_m^{CRSA} = RandSel(P_{Comm\,m_{RSA}}^{Prob\ m}, t)$

VII. $Param\_Q_m^{CRSA} = RandSel(Q_{Comm\,m_{RSA}}^{Prob\ m}, t)$

VIII. $PARAM\_P = PARAM\_P \cup Param\_P_m^{CRSA}$

IX. $PARAM\_Q = PARAM\_Q \cup Param\_Q_m^{CRSA}$

X. End For Each

The function $Split(X, Y)$ represents a splitting function that obtains the most significant bits and least significant bits of the number Y of length X. $GetPrimeSet(X)$ represents a function that uses the Sieve of Eratosthenes Prime number generation algorithm to obtain the prime numbers set within X. $RandSel(X, t)$ represents a random element in the set X selection function based on the seed time t. The communication overheads of this algorithm is $m \times 2D$ transmissions where D represents the size of the messages parsed between the m group members.

To construct the commutative RSA secure plane all the m members of the group G require a common $Param\_P_p^{CRSA}$ and $Param\_Q_q^{CRSA}$ to derive their encryption and decryption keys. A time synchronization function φ_T is adopted to ascertain the $Param\_P_p^{CRSA} \in PARAM\_P$ and $Param\_Q_q^{CRSA} \in PARAM\_Q$ amongst the group G. The time synchronization function φ_T can be considered as a $RandSel$ function wherein the seed time is common for all the members $g_m \in G$. The time synchronization function can be defined as

$\varphi_T(X, t_T) = RandSel(X, t_T)$

Where t_T represents the synchronization seed and $\forall\, g_m \in G : t = t_T$.

The time synchronization function φ_T is used to obtain $Param\_P_p^{CRSA}$ and $Param\_Q_q^{CRSA}$ defined as

$Param\_P_p^{CRSA} = \varphi_T(PARAM\_P, t_T)$

$Param\_Q_q^{CRSA} = \varphi_T(PARAM\_Q, t_T)$

The encryption and decryptions keys are to be derived from $Param\_P_p^{CRSA}$ and $Param\_Q_q^{CRSA}$ using the following algorithm

Algorithm Name: Encryption and Decryption Key Pair Computation

Input:

I. Group Member Set $\boldsymbol{G} = \{\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3}, \dots \dots \boldsymbol{g_m}\}$

II. $\boldsymbol{Param\_P_p^{CRSA}}$

III. $\boldsymbol{Param\_Q_q^{CRSA}}$

Output:

I. Encryption Key Pair $\left(\boldsymbol{Param_{N_{g_m}}}^{\boldsymbol{CRSA}}, \boldsymbol{Param_{E_{g_m}}}^{\boldsymbol{CRSA}}\right)$

II. Decryption Key Pair $\left(\boldsymbol{Param\_N_{g_m}}^{\boldsymbol{CRSA}}, \boldsymbol{Param\_D_{g_m}}^{\boldsymbol{CRSA}}\right)$

Algorithm

I. For Each group member $g_m \in G$

II. Compute $Param_{N_{g_m}}{}^{CRSA} = \left[\left(Param_{P_p}{}^{CRSA}\right) \times \left(Param_{Q_q}{}^{CRSA}\right)\right]$

III. Compute $Param_{\phi_{g_m}}{}^{CRSA} = \left[\left(Param_{P_p}{}^{CRSA} - 1\right) \times \left(Param_{Q_q}{}^{CRSA} - 1\right)\right]$

IV. Select random number using $RandSel(Rnd_{Num}, t) \mid \mathcal{F}n_{GCD}(Rnd_{Num}, Param\_\phi^{CRSA} =) 1$

V. $Param\_E_{g_m}{}^{CRSA} = Rnd_{Num}$

VI. Compute $Param_{D_{g_m}}{}^{CRSA} = \left[\left(Param_{E_{g_m}}{}^{CRSA}\right)^{-1} Mod\left(Param_{N_{g_m}}{}^{CRSA}\right)\right]$

VII. Encryption key pair of the $g_m{}^{th}$ group member is $\left(Param_{N_{g_m}}{}^{CRSA}, Param_{E_{g_m}}{}^{CRSA}\right)$

VIII. Decryption key Pair of the $g_m{}^{th}$ group member is $\left(Param_{N_{g_m}}{}^{CRSA}, Param_{D_{g_m}}{}^{CRSA}\right)$

IX. End For Each

Global Journal of Computer Science and Technology (E) Volume XII Issue XVI Version I Year 2012

Using the Encryption and Decryption Key Pair Computation algorithm all the group members $g_m \in G$ compute the encryption and decryption key pairs which enable to construct the envisioned secure communication plane. The $RASCP$ discussed eliminates the security arising from key exchange [14], negating key compromise [15] external server maintenance for key management [16] proving the efficiency in creating a secure communication plane.

Let us consider n users of the group G that need to communicate securely and the secure communication group $\bar{G}$ is defined as

$$\bar{G} = \{g_1, g_2, g_3, \dots \dots . g_n\}$$

Where $n \leq m$ and $\bar{G} \subseteq G$

The secure communication plane consisting of n group members communicate data by using a series of encryption and decryption operations. The commutative nature of the RSA algorithm adopted in the $RASCP$ ensures that the data communicated is encrypted at least once i.e. the original data is encrypted and then only communicated over the plane thereby securing the data. The presence of any colluded users within the group represented by g_c, on intercepting the data would not be unable to determine the level of encryptions and decryption procedures performed on the data prior to his interception. In the case if the user $g_c \in G$ intercepts the data after the first encryption, g_c would not be able to recover the data as the encryption and the decryption keys are not exchanged and are different for each user $g_n \in \bar{G}$ participating in the secure group communication. Let $g_{Sndr} \in \bar{G}$ represents the sender who needs to communicate data X to $g_{Rcv} \in \bar{G}$ in the presence of group member set $\bar{G}$ securely. Let us define a set $\bar{\bar{G}}$ and $\acute{G}$ as follows

$\bar{\bar{G}} = \bar{G} \cap g_{Rcv}$

$\acute{G} = \bar{G} \cap g_{Sndr}$

The algorithm to securely communicate amongst g_{Sndr} and g_{Rcv} is mentioned below

Algorithm Name: Communication over the Secure Plane

Input:

I. Group Member Set $\bar{G}$
II. Group Member Set $\bar{\bar{G}}$
III. Group Member Set $\acute{G}$
IV. Encryption and Decryption Key Pairs of Group Member Set $\bar{G}$
V. Data to be transacted X available with $g_{Sndr} \in \bar{G}$

Output:

I. Data X available with $g_{Rcv} \in \bar{G}$

Algorithm

I. For user $g_m = g_{Sndr} \in \bar{G}$
II. Encrypt the data $Enc_{g_{Sndr}} = \left[X^{Param_{E_{g_{Sndr}}}^{CRSA}} \ Mod \left(Param_{N_{g_{Sndr}}}^{CRSA} \right) \right]$
III. $Enc_{Tmp} = Enc_{g_{Sndr}}$
IV. End For
V. For Each user $g_m \in \acute{G}$
VI. Encrypt the data $Enc_{Tmp} = \left[Enc_{Tmp}^{Param_{E_{g_m}}^{CRSA}} \ Mod \left(Param_{N_{g_m}}^{CRSA} \right) \right]$
VII. End For Each
VIII. For Each user $g_m \in \bar{\bar{G}}$
IX. For the first user
X. Decrypt the data $Dec_{Tmp} = \left[Enc_{Tmp}^{Param_{D_{g_m}}^{CRSA}} \ Mod \left(Param_{N_{g_m}}^{CRSA} \right) \right]$
XI. End For
XII. Decrypt the data $Dec_{Tmp} = \left[Dec_{Tmp}^{Param_{D_{g_m}}^{CRSA}} \ Mod \left(Param_{N_{g_m}}^{CRSA} \right) \right]$
XIII. End For Each
XIV. For user $g_m = g_{Rcv} \in \bar{G}$
XV. Decrypt to get final data $X = \left[Dec_{Tmp}^{Param_{D_{g_m}}^{CRSA}} \ Mod \left(Param_{N_{g_m}}^{CRSA} \right) \right]$
XVI. End For

Using the Communication over Secure Plane Algorithm discussed above the g_{Rcv} is able to receive the data X sent by the user g_{Sndr} using n number of encryption and decryption functions. The algorithm also highlights the fact that the data X to be transmitted is not transmitted in the original form i.e. it is encrypted and transmitted there by securing the data.

The $RASCP$ discussed utilizes the $RFID$ tags available with each group member g_m to construct the secure communication plane. The *RFID* tags are often used for identification and tracking. In $RASCP$ the RFID tags are used both for security provision and identification. As the $RASCP$ adopts multiple encryption and multiple decryptions to securely communicate data the overheads arising from this could be considered as a drawback of the $RASCP$. The $RASCP$ is evaluated with the Secure Lock secure group communication protocol in the subsequent section of this paper.

V. RFID EXTENDED SECURE LOCK GROUP COMMUNICATION SCHEME (RSL)

The RSL is a $RFID$ based extended Secure Lock protocol [17]. The RSL protocol considers a central server and a set of group members defined as $G^{RSL} = \{g_1^{RSL}, g_2^{RSL}, g_3^{RSL}, \dots \dots . g_m^{RSL}\}$

The RSL protocol incorporates an asymmetric cryptographic algorithm to provide security. Let the private and public of a group member $g_m{}^{RSL} \in G^{RSL}$ be represented as $(\mathcal{P}^{RSL}{}_m, \mathcal{S}^{RSL}{}_m)$.

The central server also known as the security server establishes a set of $m = |G^{RSL}|$ pair wise relatively prime numbers $\mathcal{N}_1, \ldots, \mathcal{N}_m$ from the $RFID$ tags possessed using the Sieve of Eratosthenes Prime number generation algorithm. These numbers are then assigned to group members $g_m{}^{RSL} \in G^{RSL}$ and are assumed to be public in nature. To establish a secure plane of for communication using the RSL the server computes the following based on the a randomly selected key represented as K^{RSL}

$$\mathcal{Lck}^{\mathrm{RSL}} \equiv \mathcal{E}_{\mathcal{P}^{RSL}{}_m}(K^{RSL})(\mathcal{mod}\ \mathcal{N}_{m^{RSL}})$$

Where $\mathcal{E}$ represents the encryption operation

Using the Chinese remainder theorem the server computes $\mathcal{Lck}^{RSL}$. The computed value $\mathcal{Lck}^{RSL}$ is considered as the lock for the key $\mathcal{E}_{\mathcal{P}^{RSL}{}_m}(K^{RSL})$ .The resulting message sent by the server is defined as

$$\mathcal{msg}^{RSL}{}_m = \left(\mathcal{Lck}^{RSL}, \{K^{RSL}\}_{K^{RSL}}\right)$$

The group member $g_m{}^{RSL}$ on receiving the message $\mathcal{msg}^{RSL}{}_m$ obtains the $\mathcal{Lck}^{RSL}$ using the following computations

$$\mathcal{E}_{\mathcal{P}^{RSL}{}_m}(K^{RSL}) = (\mathcal{Lck}^{\mathrm{RSL}})\ (\mathcal{mod}\ \mathcal{N}_{m^{RSL}})$$

$$K^{RSL} = \mathcal{D}_{\mathcal{P}^{RSL}{}_m}\left(\mathcal{E}_{\mathcal{P}^{RSL}{}_m}(K^{RSL})\right)$$

Where $\mathcal{D}$ represents the decryption operation.

Colluded group members on decryption cannot obtain the lock K^{RSL} selected by the server accurately hence providing for security.

The Chinese remainder theorem utilized by the server provides protection by securing the group membership and group size. The use of the Chinese remainder theorem and asymmetric cryptographic schemes render the RSL group communication scheme inefficient and are not scalable.

VI. Performance Evaluation

This $RASCP$ secure communication mechanism proposed in this paper is compared with the RSL protocol in terms of the computational costs incurred. The computational cost incurred is proportional to the execution time observed. The $RASCP$ and the RSL systems were developed using C#.Net on the Visual Studio 2010 Platform. The $RFID$ tags used were of type 0. The $RFID$ readers were integrated into the platform using VC++.Net. To evaluate the $RASCP$ and the RSL secure group communication systems and to observe the computational costs the number of users in the group were varied from 5, 10, 20, 50, 70 and 100 users. The observations were monitored using log files maintained for every operation. The introduction of the $RFID$ tags into the $RASCP$ and RSL can be considered as an overhead that exists in reading the tags and the average time observed in reading the RFID tags when the number of group members are varied from 5, 10,20,50,70 and 100 is as shown in Fig 1. It could be observed that the average of the overheads observed reduces as the number of users increase proving that the induction of the $RFID$ based security systems are scalable in nature and do not affect the responsiveness of the systems. The average time taken to read a $RFID$ tags was found to be about 0.76ms.

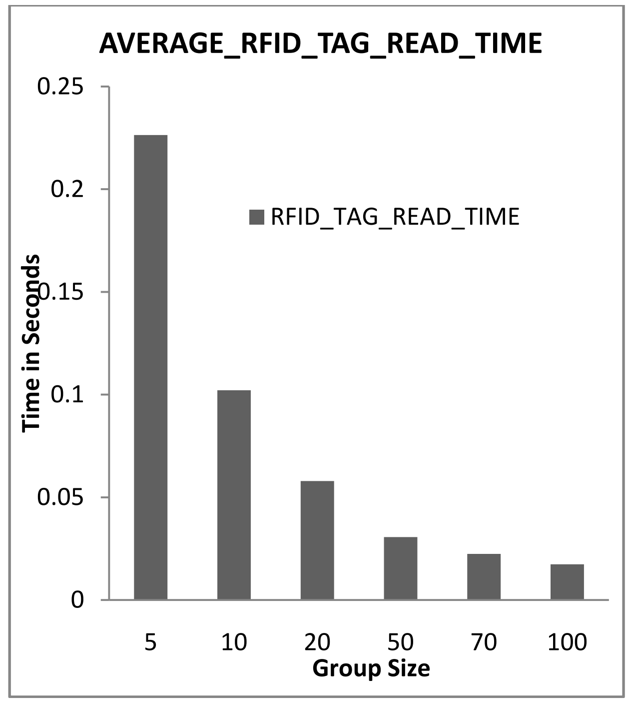

Figure 1 : Average Time Observed in Reading RFID Tags with Varying Number of Group Members

The RSL secure group communication system adopts the RSA Algorithm with a key strength of 1024 [19] bits to incorporate secure transmissions amongst the group members. The $RASCP$ adopts the commutative RSA algorithm to construct a secure communication plane. The RSL relies on a central server for key initialization, distribution using locks and the verifications is carried out by the group members. The experimental evaluation conducted considered the protocol initialization phase as the time taken to verify the group membership and derive the cryptographic keys. The computational overheads observed are as shown in Fig.2. It could be observed that the overheads are reduced by about 99.43% in the initialization phase in the $RASCP$ protocol. The RSL considers a central server and the verification process of the group members. The overheads resulting from the group membership verification process for the RSL scheme is as shown in Fig 3. The $RASCP$ and the RSL group communication protocols adopt cryptographic techniques to construct a secure communication plane.

The overheads arising from the encryption and decryption operations are analyzed for comparisons. The encryption and decryption operations performed using the $RASCP$ and the RSL group communication schemes are compared in terms of the computational complexity exhibited. The results obtained are graphically shown in Fig 4 and Fig 5. Form the figures it is clear that the commutative RSA algorithm adopted in the $RASCP$is computationally less expensive when compared to the RSA cryptographic algorithm adopted in the RSL group communication scheme ye providing security.

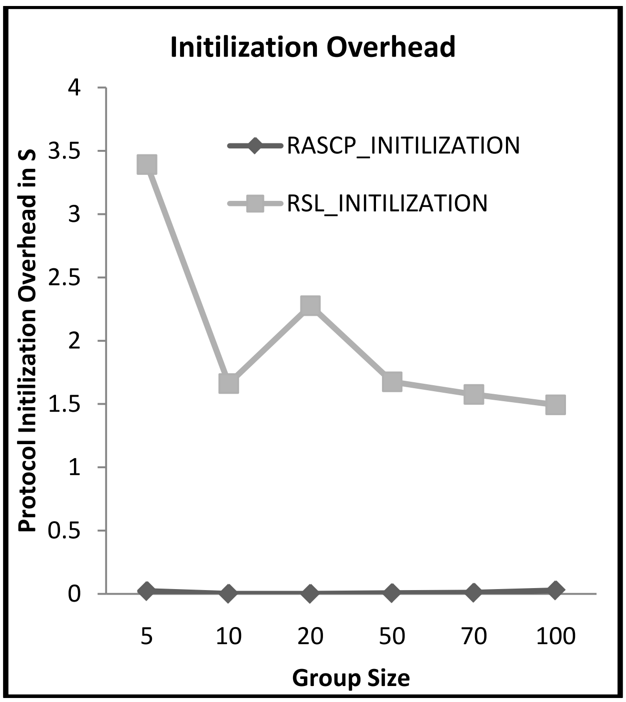

Figure 2 : Average Protocol Initialization Overheads Vs Group Size

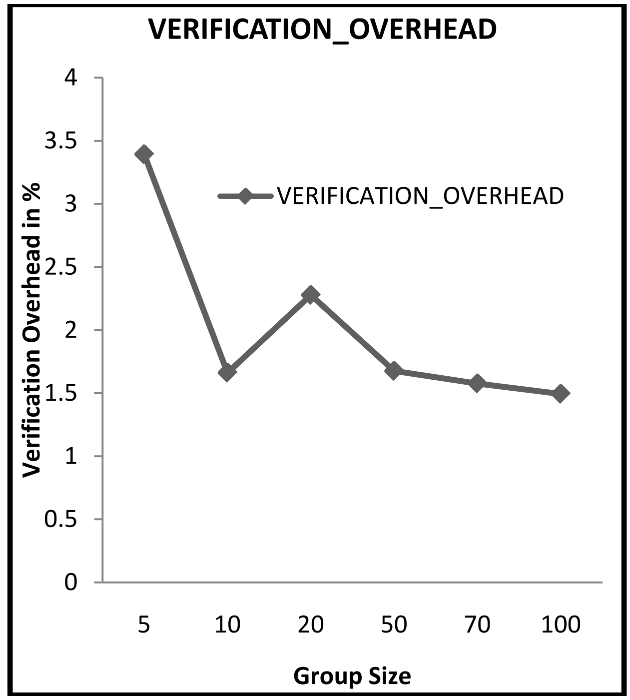

Figure 3 : Verification Overhead in RSL Scheme

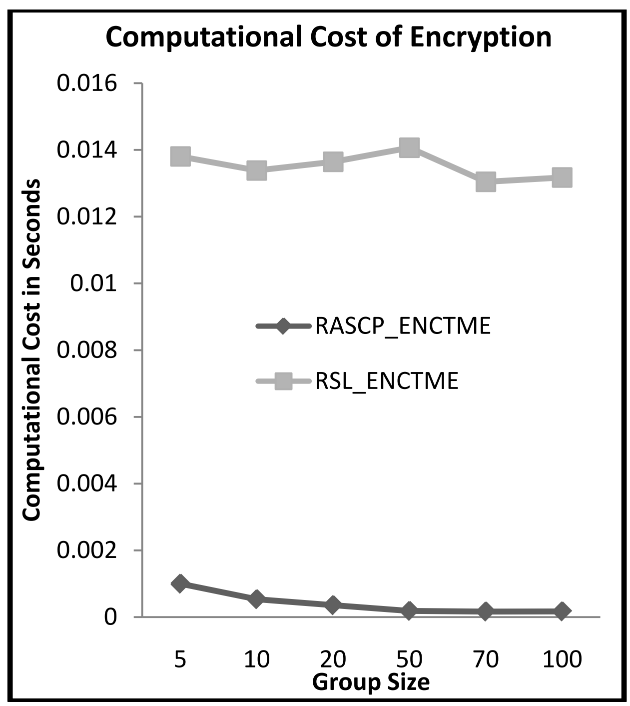

Figure 4 : Computational Analysis of Encryption Operations

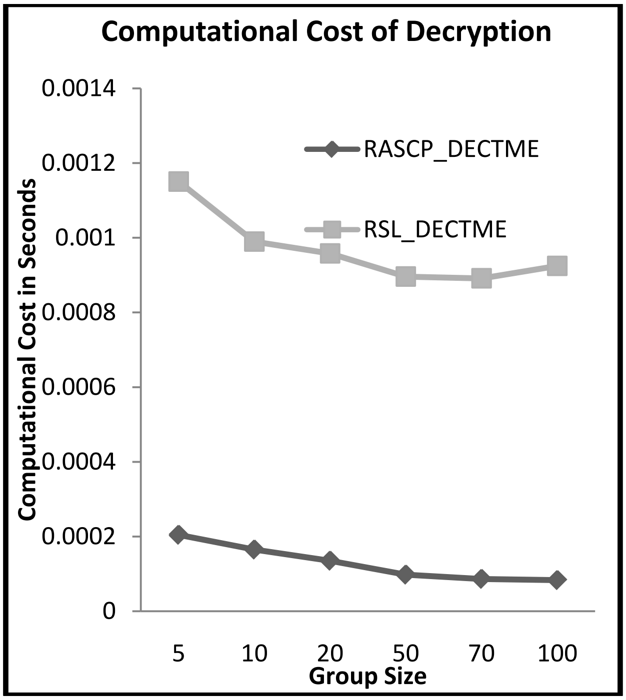

Figure 5 : Computational Analysis of Decryption Operations

The experimental evaluation discussed in this paper prove that the proposed *RASCP* group communication protocol introduced in this paper performs better than the existing *RSL* scheme by reducing the computational overheads and yet providing security of the data transacted amongst the group members.

VII. Conclusion and Future Work

RFID devices are universally used for the purpose of identifications. Many researchers have focused on improving the security of RFID systems in place. This paper introduces a RFID Authentication based Secure Communication Plane (*RASCP*) felicitating secure transmissions amongst group members. The *RASCP* protocol adopts the commutative RSA algorithm to preserve the integrity of the data transacted over the communication plane. The RFID tags are used for the purpose of identification and for protocol initialization. The proposed *RASCP*scheme is compared with the *RSL* secure group communication scheme. The *RASCP* scheme proposed overcomes the drawbacks arising from key distribution, key compromise and external trusted server requirements, yet providing security in the presence of even colluded users. The experimental study conducted proves the efficiency of the proposed *RASCP* over the *RSL* group communication scheme.
The future of the work presented here is to compare the RASCP scheme with other secure group communication schemes using RFID tags.

References Références Referencias

1. IEEE-SA Standards Board,"IEEE Standard for Smart Transducer Interface for Sensors and Actuators—Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet Formats" , IEEE Instrumentation and Measurement Society.IEEE Std 1451.7TM-2010
2. INTERNATIONAL STANDARD"Transducer to radio frequency identification (RFID) systems communication protocols and Transducer Electronic Data Sheet (TEDS) formats" ISO/IEC/IEEE21451-7,First edition 2011-12-15
3. S. Weis, “Security and Privacy in Radio-Frequency Identification Devices,” master’s thesis, Mass. Inst. of Technology (MIT), May 2003
4. Basel Alomair, Andrew Clark,Jorge Cuellar, and Radha Poovendran,"Scalable RFID Systems: A Privacy-Preserving Protocol with Constant-Time Identification",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL. 23, NO. 8, AUGUST 2012,pp 1536 - 1550
5. H. Lee and J. Kim, “Privacy Threats and Issues in Mobile RFID,” Proc. First Int’l Conf. Availability, Reliability and Security (ARES ’06), Apr. 2006
6. A. Juels, “RFID Security and Privacy: A Research Survey,” manuscript, RSA Laboratories, Sept. 2005.
7. D. Molnar and D. Wagner, “Privacy and Security in Library RFID: Issues, Practices, and Architectures,” Proc. 11th ACM Conf. Computer and Comm. Security (CCS ’04), Oct. 2004.
8. S. Weis et al., “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems,” Proc. First Int’l Conf. Security in Pervasive Computing (SPC ’03), Mar. 2003.
9. A. Juels, “Minimalist Cryptography for Low-Cost RFID Tags,” Proc. Fourth Int’l Conf. Security in Comm. Networks (SCN ’04), Sept. 2004.
10. Y. J. Huang, C. C. Yuan, M. K. Chen, W. C. Lin, and H. C. Teng, “Hardware implementation of RFID mutual authentication protocol,” IEEE Trans. Ind. Electron., vol. 57, no. 5, pp. 1573–1582, May 2010.
11. D. Gries and J. Misra. A linear sieve algorithm for finding prime numbers. Communications of the ACM, 21(12):999–1003, 1978
12. Gabriel Paillard,"A FULLY DISTRIBUTED PRIME NUMBERS GENERATION USING THE WHEEL SIEVE",Parallel and Distributed Computing and Networks, 2005 pp651-656
13. R. Crandall and C. Pomerance. Prime Numbers: a computational perspective. Springer Verlag, 2001
14. Victor P. Hubenko Jr., Richard A. Raines, Rusty O. Baldwin, Barry E. Mullins, Robert F. Mills, and Michael R. Grimaila,"Improving Satellite Multicast Security Scalability by Reducing Rekeying Requirements",IEEE Network • July/August 2007, pp 51-56

15. Bezawada Bruhadeshwar and Sandeep S. Kulkarni,"Balancing Revocation and Storage Trade-Offs in Secure Group Communication ",IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 1, JANUARY-FEBRUARY 2011 pp58-73
16. Nathaniel Karst, and Stephen B. Wicker,"On the Rekeying Load in Group Key Distributions Using Cover-Free Families ",2011 IEEE.
17. G. H. Chiou and W. Chen, “Secure broadcasting using the Secure Lock,” IEEE Transactions on Software Engineering, vol. 15, no. 8, pp. 929–934, Aug. 1989.
18. Xukai Zou, Mingrui Qi, and Yan Sui."A New Scheme for Anonymous Secure Group Communication",System Sciences (HICSS), 2011 44th Hawaii International Conference.4-7 Jan. 2011.
19. Arjen K. Lenstra, Key length. Handbook of Information Security, Editor-in-Chief, Hossein Bidgoli, pp 617–635.