Exponentiated Multiple Message Communication using Certificateless Signcryption for Mobile Network Security

Sumithra Alagarsamy
Part Time Research Scholar
Dept of Information and Communication Engineering
Anna University Chennai, Tamil Nadu, India

S. P. Rajagopalan
Professor/CSE,
G.K. M. College of Engineering
Tamilnadu, India

ABSTRACT
The rapid progress in the internet requires multiple message communication over the wider area to improve the mobile network security. Due to the multiple message communication, the security is a most important concern in mobile network. The bilinear Certificate less Aggregate Signcryption Scheme guarantees the security under several attacks, and therefore provides security and non-repudiation. However, the multiple messages through a single operation are a difficult task to improve the network security. In addition, multilinear map based signcryption scheme provides the confidentiality and authenticity but it is complicated for handling when number of messages gets increased rapidly. In order to overcome the problem in multiple message communication, Exponentiated Multilinear Vectorized Certificateless Signcryption (EMV-CLSC) technique is introduced. The EMV-CLSC technique is used to verify the multiple messages through a single Signcryption process. An efficient certificate less signcryption technique performs the multiple message communication between senders andreceiver to ensure the network security. In EMV-CLSC, the multilinear vectorized model is applied for handling the high volume of data and multiple data format while distributing the message simultaneously. This helps to reduce the memory consumption while processing the multiple data. The proposed EMV-CLSC technique provably improves the security with public key verifiability and cipher text authenticity. Based on, the authorized users only access the network and the messages are protected. At last, the Broadcast message is secured using Digital Signature verification in uncsigncryption process. A certificate less signcryption process with multiple bits is used to highly secure the multiple messages using EMV-CLSC technique. This helps to protect the messages against the attacks and improve the mobile network security. An experimental result shows that the proposed EMV-CLSC technique improves the network security in terms of computational cost, memory consumption, communication overhead and secured message distributing rate compared to the state-of-the-art works.

Keywords
Mobile network security, Certificateless scheme, Signcryption, Multilinear vectorized model, multiple message communication, signature verification.

1. INTRODUCTION
A mobile network consists of the several mobile nodes which are wirelessly connected to the internet through the mobile operator. Due to the increasing demand of the internet, the security is major concern during the simultaneous message broadcasting. In order to improve the mobile network security, there are several cryptography schemes were developed. As a result, the security aspects have to be considered so that message broadcasting can be executed in an efficient manner.

An efficient certificateless signcryption scheme was developed in [1] by using an access control scheme for the WBANs using the given signcryption. This scheme achieves confidentiality and integrity. However, the multiple messages through a single operation are a difficult task to improve the network security.

A new Identity-based certificateless aggregate signcryption scheme was developed in [2] to improve the confidential and unforgeable under the assumption of multilinear Diffie-Hellman problem in the standard model. However, it is complicated for handling the more messages gets increased rapidly.

A new mutual authentication and key management mechanisms were introduced in [3] for smart grid communications. In [4], a secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol improves the security performance.

An attribute-based encryption scheme was developed in [5] for fine-grained access control in WBANs and it provides confidentiality, security and minimum energy consumption. A new security model was designed in [6] to describe proxy signcryption scheme depends on the security model. However, the overall communication cost is not reduced at the required level during the signcryption process. A new security algorithm is presented in [7] with the combination of both symmetric and asymmetric cryptographic techniques for improving the high security with minimum key maintenance.

A new security method called as Fuzzy Attribute-Based Signcryption (FABSC) was developed in [8], which create a perfect arrangement between security and elasticity. However, it requires more computation cost and storage requirements. In [9], Certificate less Cryptography technique was developed for ensuring authenticity and revocability of Wireless Body Area Network. An energy efficient method was introduced in [10] for securely and reliably transmitting messages from the sensor nodes to the medical server and improves the overall reliability of the system.

The contribution of the research work is categorized as follows. With the rapid development of internet, mobile network security is plays a significant part in multiple message broadcasting. The Exponentiated Multilinear Vectorized Certificateless Signcryption (EMV-CLSC) technique is introduced to improve the mobile network security with multiple message distributing. The certificate less Signcryption technique performs both the encryption and signature verification. The encryption process is used to

convert the plain text into cipher text with the sender private and secret key. After that, the receiver obtains the plain text with their private key. Finally, the digital signature is verified in order to enhance the security of the mobile network.

The rest of this paper is categorized as follows: Section 2 presents a brief introduction of related works. Section 3 describes the Exponentiated Multilinear Vectorized Certificateless Signcryption (EMV-CLSC) technique with neat diagram. In Section 4, the simulation environment is presented and the simulation results are obtained in section 5. Finally, the concluding remarks are explained in section 6.

2. RELATED WORKS

In [11], two public key based algorithms RSA and Elliptic Curve Cryptography (ECC) were developed for reducing the computation time and also reduces the storage space. A new efficient key management scheme was introduced in [12] based on Elliptic Curve Cryptography (ECC) and AVL tree for large scale WSNs and reduce the memory and computational overhead. However, the key update is not supports for guaranteeing the security of WSN. The symmetric key cryptography technique was introduced in [13] for both encryption and decryption in the field of network security.

An improved security model of certificate-based signcryption was designed in [14] that cover both public key alternate attack and insider security. However, the security is achieved only in the random oracle model. In [15], the various approaches were used in cryptography for Network security purpose but the key management and optimal cryptography algorithm was remained unaddressed.

In [16] the two certificate less short multi signature schemes were designed using elliptic curve and bilinear pairing to improve the network security but it suffer from the execution of costly elliptic. A new cryptography algorithm was introduced in [17] depends on exclusive-OR function to enhance data security.

Software-Defined Mobile Network (SDMN) architecture was designed in [18] in order to improve the security advantages. A Cluster-based Certificate Revocation with Vindication Capability (CCRVC) scheme was designed in [19] to improve the secure communications in mobile ad hoc networks. An enhanced secure sensor association and key management protocol based on ECC and hash chains was developed in [20] to present secure and correct association of a group of sensors and improve the data confidentiality and integrity in Body area networks (BANs).

Based on the above mentioned methods and techniques, an efficient Exponentiated Multilinear Vectorized Certificateless Signcryption technique is developed for secured multiple message broadcasting between sender and receiver in mobile network. The next section is clearly defined that the proposed secured model with the help of neat diagram.

3. EXPONENTIATED MULTILINEAR VECTORIZED CERTIFICATELESS SIGNCRYPTION TECHNIQUE

The signcryption is a novel public key cryptographic technique which uses an Encrypt-then-Sign approach in order to improve the mobile network security. Encryption and digital signature are two basics cryptographic tools that used to ensure the confidentiality, integrity, and non-repudiation with a minimum computational cost followed by encryption approach. In addition, signcryption is a public-key primitive that used to perform the functions of both digital signature and encryption. In public key cryptography, there are multiple senders and receivers are presented with the number of public-private key pairs. Therefore, the numbers of messages are increases exponentially. In order to handle the multiple images, the proposed EMV-CLSC technique uses the multilinear vectorized model. This multilinear vectorized model is a function of more than a few variables that is linear divided in each variable. The proposed Exponentiated Multilinear Vectorized Certificateless Signcryption (EMV-CLSC) technique achieves confidentiality and authentication by combining public-key encryption and digital signatures verification in order to obtain the minimum computation cost and communication overhead.

A secure and efficient EMV-CLSC technique ensures that the each message 'm' to be sent to the receiver, a public, private key pair is generated for each sender-receiver pair. The key generation is based on the certificateless signcryption algorithm. The proposed EMV-CLSC technique requires single signcryption operation to perform multiple message bits to highly secure the broadcasted message in network. Figure 1 given below shows the flow model for Exponentiated Multilinear Vectorized Certificateless Signcryption (EMV-CLSC) technique.

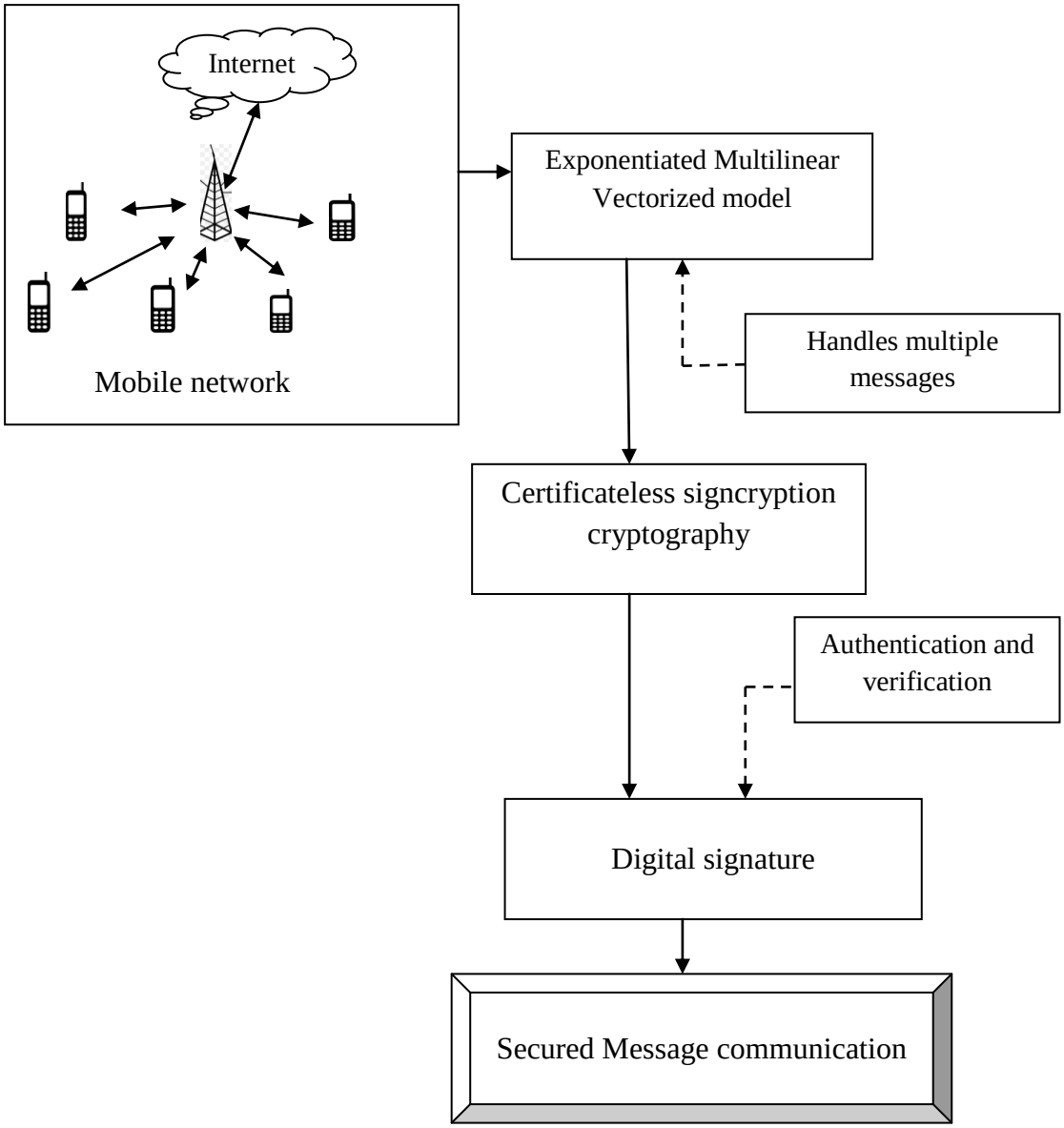

Figure 1 Flow process of Exponentiated Multilinear Vectorized Certificateless Signcryption Technique

Figure 1 shows the secure message broadcasting through Certificateless signcryption model using identity based Cryptography with the main objective of improving the mobile network security. In mobile network, the number of message broadcasting is done with the help of Exponentiated Multilinear Vectorized model. The proposed technique considers more messages being broadcasted from sender to receiver by use of vectors where one symbol represents several messages. Therefore it also helps to handle the multiple data format while concurrently distributing the messages in mobile network and also reduce the memory consumption.

Let us considers the number of messages $m_{1,}m_2 \ldots . m_n$. the maximum message bits are stored by the vector is formularized as,

$$Max\ U(m_{1,}m_2 \ldots . m_n) \quad (1)$$

While broadcasting the messages from sender to receiver, the security is the significant part in network. Therefore the certificateless signcryption techniques are applied for secured message communication with the help of vectorized model. The brief explanation about the EMV-CLSC technique is presented in forthcoming section.

3.1 Certificate less Signcryption (CLSC) Technique for Network Security

The proposed EMV-CLSC technique requires that the sender in certificate less environment to transmit a message to a receiver through identity based cryptography. The certificate less cryptography also used to reduce the key escrow problem. It is a key exchanging process in which the key is stored by third party. Under the circumstances, the key is only used for sender and receiver to encrypt the date for improving the network security. Therefore, this helps to reduce the unauthorized user access the messages in mobile network.

Let us considered the sender who is in the internet host, while the receiver in the mobile node. Generally, a signcryption scheme consists of three process such as Key Generation (Gen), Signcryption (SC), and unsigncryption (USC). In Key Gen Generation, a pair of keys is generated for any user who is contributed in signcryption process. The Signcryption is

usually a probabilistic algorithm and it is used to create the cipher text according to the plaintext depends on both public and private keys. Finally, the USC is the deterministic and it is used to decrypt the plain text (i.e original messages) from cipher text. The general process of the signcryption technique is explained as follows.

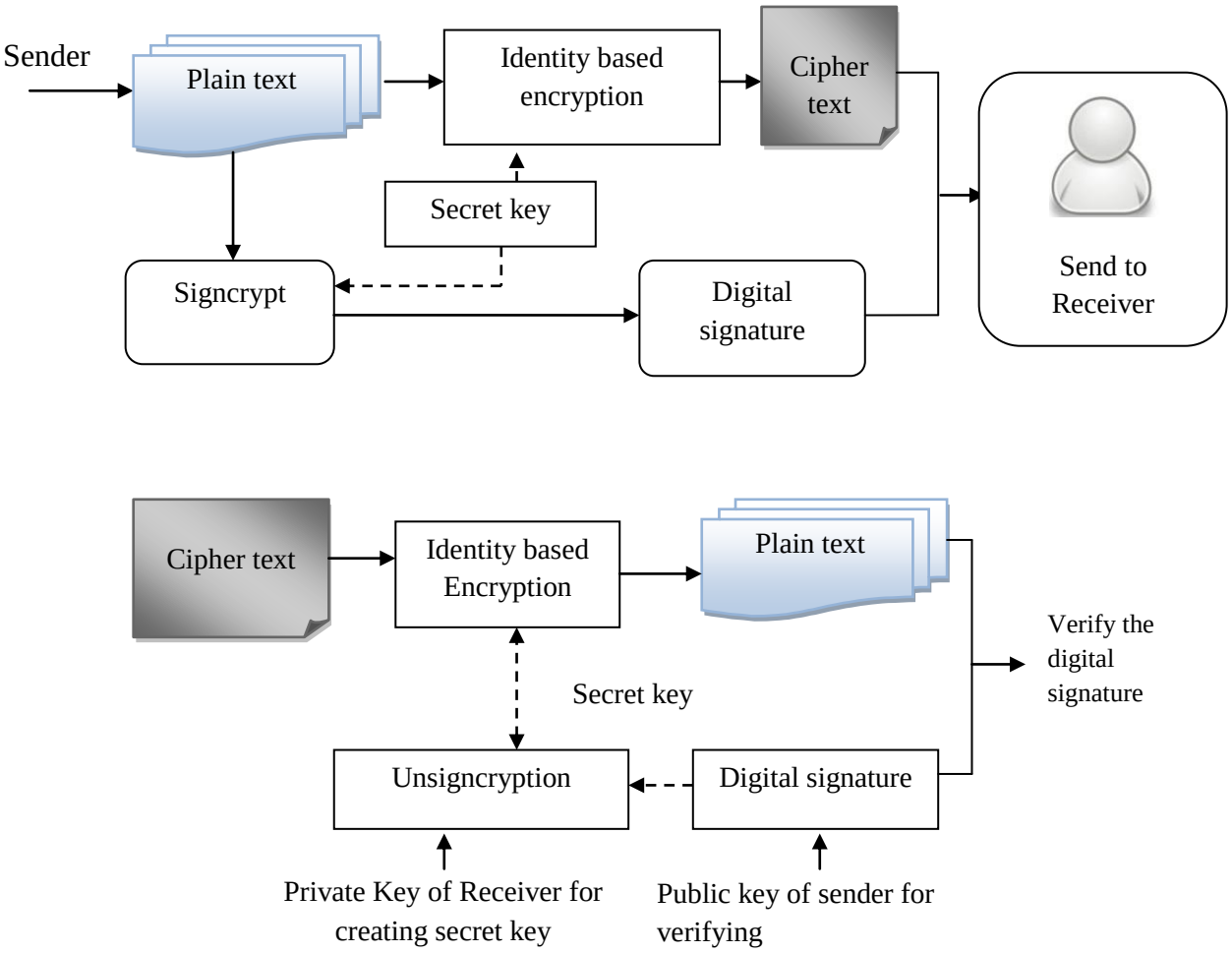

Figure 2 General Block Diagram of Signcryption Processes

The above figure 2 clearly illustrates that the signcryption process which performs both the signcryption and digital signature simultaneously. From the figure, the input messages (i.e. plain text) are encrypted using the identity based cryptographic technique to convert the cipher text. Simultaneously, the digital signature process is carried out for transmitting the message to the receiver.

In the signcryption process, the cryptography technique uses the secret key for encrypt the message. The certificate less cryptography technique provides more benefits such as higher security, high speed, minimum storage space and less bandwidth. The identity based scheme where any user's public id similar to email address, MAC address are used as a public key that reduces the key management issue. This helps to reduce the computational cost.

In certificateless cryptography, the trusted third party (i.e. TTP) is also known as Key Generation Center (KGC). The TTP provides the user with a partial private key which it evaluates from the user's identity (ID) and a master key. It is essential; the TTP is required to distribute the partial private keys to the user in a secure manner. The Identity-based system permits the user to generate a public key from a well-known identity value. A trusted third party generates the equivalent private keys. Initially, the private key generator (PKG) distributes a master public key, and maintains the related master private key. By grouping the master public key through the identity value, the user calculates a public key related to the identity ID. The authorized user employs the ID associates the PKG for accessing the messages in mobile networks to obtain a corresponding private key. This helps to reduce the unauthorized user to access the distributed messages. The secure message communication is carried out as shown in figure 3.

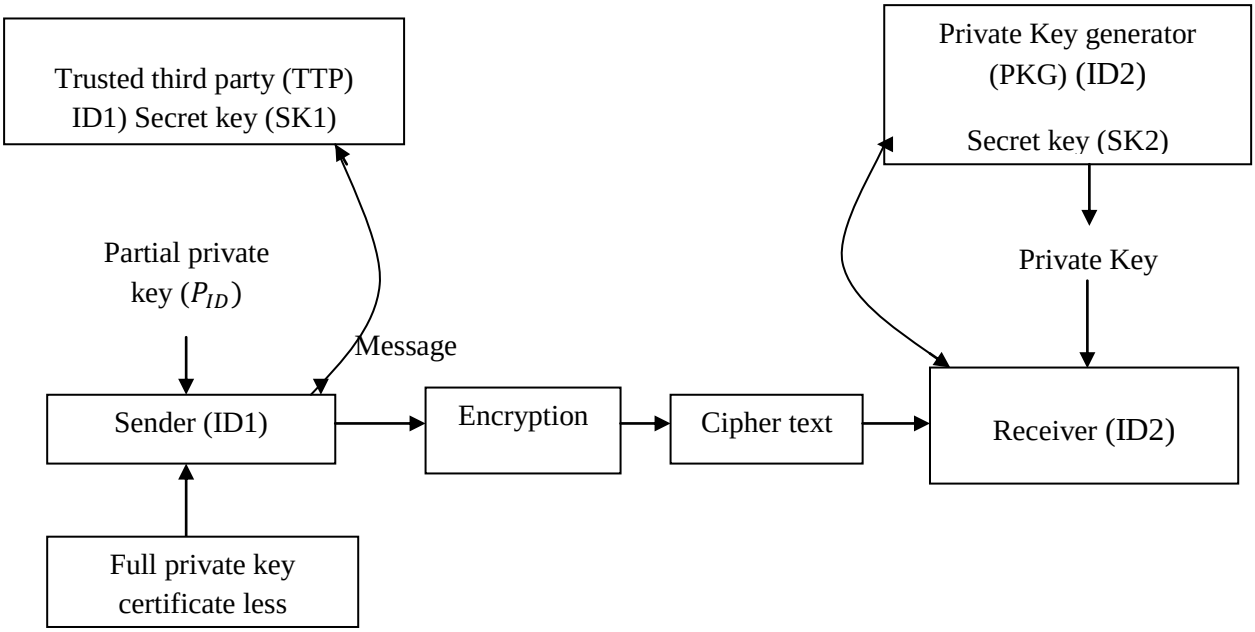

Figure 3 Secured message communications between sender and receiver

Figure 3 illustrates the secured message distribution between sender and receiver based on private key and public key extraction. The proposed EMV-CLSC technique is specified by seven processing step in order to create the Certificateless Signcryption algorithm such as Setup phase, Partial private key extraction , Generate user key , Set full private key, Extract-key- identity based cryptography, Signcryption and unsyncryption.

Step 1: Setup phase,
In Setup phase, Considers the input security parameter K and outputs of the system parameters (P) and a master secret key msk1 and msk2 . The TTP and PKG runs these setup algorithm to attain the secrete keys SK1 and SK2 and also proceeds a global system parameters with representing the master public keys of TTP and PKG respectively. Then the TTP selects the multilinear group $GR_1, GR_2 \ldots . GR_n$ which is generated by additive group (AG). The four certificates less cryptographic hash function (HF) are used to perform the secure communication.

$$HF_1: \{0,1\}^* \rightarrow GR_1$$
$$HF_2: \{0,1\}^* \rightarrow \{0,1\}^K$$
$$HF_3: \{0,1\}^* \rightarrow GR_1$$
$$HF_4: \{0,1\}^* \rightarrow GR_1$$

While the number of input messages increases exponentially, the PKG selects the random vector $U = u_1, u_2, \ldots . u_n$ and $V = v_1, v_2, \ldots . v_n$. These two vectors are used to handle the multiple messages simultaneously distributed to the receiver. The vector elements are selected randomly from the multi linear group GR_1. The TTP selects the random value 'r'. The public parameters $< GR_1, GR_2, p, e, P_{pub}, g, HF_1, HF_2 HF_3, HF_4 >$ are used to perform the signcryption.

Step 2: Partial private key extraction
A user in the certificate less environment submits as identity ID to an algorithm run by TTP which take as input value Master secret key and Parameters (P), while the user identity is $U_{ID} \in \{0,1\}^*$. Therefore, the TTP sets the partial private key which is described as,

$$PPR_{ID} = SK_1 \, HF_1 \, (ID) \quad (2)$$

The hash function of user Identity $HF_1 \, (ID)$ and secret key SK_1 is used for extracting the partial private key in a secure manner.

Step 3: Generate user key
In signcryption, the private and public keys are generated by the cryptography method makes the message bits more secure for establishing and also the generating keys are robust. The conventional key generation and construction techniques were developed to improve the confidentiality and integrity. However, the multilinear message transmission is major task in mobile networks. In order to overcome the above limitation, Exponentiated Multilinear Vectorized model based Certificateless Signcryption technique is introduced in mobile network.

In the private key and public key generation, the user input Identity (ID) and it is combined with the public parameter (P) to returns the secret value. The secret value of the user identity is denoted as α_{ID} which is also used for constructing the user private key and public. The secret value of the user identity is also returns the public Key (PB_k). The secret value α_{ID} and public key are used to construct the full private key.

Step 4: Set full private key
The full private key is generated in which the user submit identity (ID), secret value α_{ID} and public parameters. This is a deterministic algorithm run by the user and it is calculated as follows,

$$FPR_k = (\alpha_{ID} \, , PPR_{ID}) \quad (3)$$

Step 5: Extract-key- identity based cryptography
The user submits identity to the private key generator (PKG) whose uses the master secret key and user's to create the related private key in a secure manner.

Step 6: Signcryption

The input of the messages $m_1, m_2, \ldots m_n \in P$, sender full private key PR_{k1}, Identity ID1 and public keyPB_{k1} are used to perform the syncryption to distribute the message in secured manner with minimum overhead. From the figure3, receiver user identity is taken as ID2, public key PB_{k2} and the global parameter (p). The output of the signcryption produces the output of the cipher text (C).

$$C = (\mathrm{ID2}, PB_{k2}) \quad (4)$$

From figure 2, clearly illustrates that the syncryption process in order to convert the original message into the cipher text (C).

Step 7: Unsigncryption

The final process to be performed to improve the security is to verify the signature using Digital Signature Verification and therefore the secure message forwarding rate is increased. In proposed EMV-CLSC technique, the unsyncryption is a deterministic algorithm which utilizes the input of cipher text (c), receiver full private key PR_{k2} , Identity ID2 and public key PB_{k2} , the senders identity ID1, public key PB_{k1} and the global parameters (P). Therefore, this probabilistic algorithm takes sender public key and unsigncrypted data as input to produce an output of the algorithm as the original messages (m).

$$m = (P, PB_{k1}, \mathrm{ID1}) \quad (5)$$

From (5), the original message (m) is attained at the receiver end with the help of the public parameters and sender's public key and identity. Followed by, the proposed EMV-CLSC performs the process of digital signature verification is attained to verify the signature and improves the secure message distributing rate. The EMV-CLSC technique performs signature verification by using following if-then condition. The signature verification (ST_{ik}) through the equation given below,

$$IF\ (ST_{ik}) = (public\ key), then\ valid\ signature \quad else \quad invalid\ signature \quad (6)$$

From (6), where ST_{ik} is multi bit the digital signature, $ST_{ik} = ST_{i1}, ST_{i2}, \ldots, ST_{ik}$. A signature verifying algorithm that, given the input message, public key and signature, either accepts or rejects the messages preserves the secrecy. Finally the broadcasted message (i.e., packet) is secured in mobile network by applying the signcryption algorithm. The algorithmic procedure for the signcryption process is described as follows,

Input: Number of messages, security parameter K, sender private key PR_{k1}, receiver private key PR_{k2} , sender identity ID1, receiver identity (ID2), sender public key PB_{k1}, receiver public key PB_{k2}
Output : Secured message broadcasting in mobile network
Step 1: begin
Step 2: For each sender and messages (m)
Step 3: Extract the partial private key with identity (ID1) using (2)
Step 4: Generate the secret value $\alpha_{ID}$to construct private and public key
Step 5: Set full private key using (3)
Step 6: Perform signcryption to convert plain text cipher text (C) using (4)
Step 7: Evaluate Digital Signature Verification
Step 8: If $(ST_{ik}) = (public\ key)$ then
Step 9: Valid signature
Step 10: Else
Step 11: Invalid signature
Step 12: Unsigncrypt the cipher text (C) using (5)
Step 13: Obtain the plain text to the receiver
Step 14: End if
Step 15: End for
Step 16: End

Algorithm 1 Certificate less Signcryption algorithm

The above algorithmic procedure clearly illustrates that the certificate less signcryption procedure in order to ensure the secure message broadcasting in mobile network. The EMV-CLSC technique performs the signcrypt and unsigncrypt process with the help of private key and public key generation based on the identity (ID1). The EMV-CLSC technique uses the private key of the sender in certificate less environment for encrypting the plain text into cipher text. For handling the multiple messages broadcasting, the vectorized model is introduced in setup phase in order to reduce the memory utilization. Therefore, the unsigncryption takes as input sender's public key and cipher text to convert the plain text. Followed by, Digital Signature verification is performed through an if-then condition that performs conditional search between secret and public key accordingly, if the secret and public keys are similar, the signature is valid or else the signature is invalid. Therefore, the proposed EMV-CLSC technique effectively performs the multiple messages distribution between senders and receiver with minimum communication overhead and also improving the mobile network security.

4. SIMULATION SETTINGS

The simulation performance of the proposed Exponentiated Multilinear Vectorized Certificateless Signcryption (EMV-CLSC) technique is implemented in NS-2 simulator. The nodes were initially placed within a fixed size of 1000 m * 1000 m square area with a velocity of 0 – 50 m/s in a square area. The mobile network consists of 500 nodes in the network structure and uses the Random Way Point (RWM) model. The routing protocol used for EMV-CLSC technique uses Dynamic Source Routing (DSR) to improve the secured message communication between the sender and receiver in mobile networks. The simulations parameters are listed in table 1.

Table 1 Simulation parameter

Parameter	Value
Simulator	NS-2.31
Number of nodes	50,100,150,200,250,300,350,400,450,500
Network area	1000*1000m
Transmission range	250m
Number of messages	5,10,15,20,25,30,35,40,45,50
Simulation period	600s
node speed	2 -25m/s
Node pause time	0 – 300 seconds
Routing protocol	Dynamic source routing protocol (DSR)
Number of runs	10

5. SIMULATION RESULTS AND ANALYSIS

An Exponentiated Multilinear Vectorized Certificateless Signcryption (EMV-CLSC) technique is evaluated with the existing Certificate Less Sign Cryption (CLSC) [1] and Identity-Based Aggregate Signcryption scheme (IBASC) [2]. The experimental evaluation is carried out with the different parameters such as computation cost, Memory consumption, Communication overhead and Secured message distributing rate. Performance is measured with the help of tables and graph values.

5.1 Impact of computation cost

Computation cost is defined as the total time taken to evaluate the certificate less syncryption algorithm to run as a size of the messages representing the input. It is measured in terms of milliseconds (ms).

$$CC = Time\ (Run\ a\ certificate\ less\ syncryption\ algorithm) \quad (7)$$

From (7), Computation cost (CC) is the time taken by the algorithm to perform the efficient message broadcasting.

Table 2 Tabulation for computation cost

Message size (KB)	Computation cost (ms)		
	EMV-CLSC	CLSC	IBASC
15	22.3	28.9	32.7
30	28.4	32.8	34.9
45	32.1	40.1	42.6
60	41.8	50.2	53.6
75	46.7	55.3	58.9
90	50.1	58.6	60.1
105	52.6	60.3	63.4
120	55.7	66.1	69.7
135	60.4	69.8	72.3
150	62.3	71.2	73.6

Table 2 clearly describes the measure of Computation cost based on different size of the messages being broadcasted. The message size is represented in terms of KB. The proposed method EMV-CLSC technique reduces the communication cost compared to existing Certificate Less Sign Cryption (CLSC) [1] and Identity-Based Aggregate Signcryption scheme (IBASC) [2].

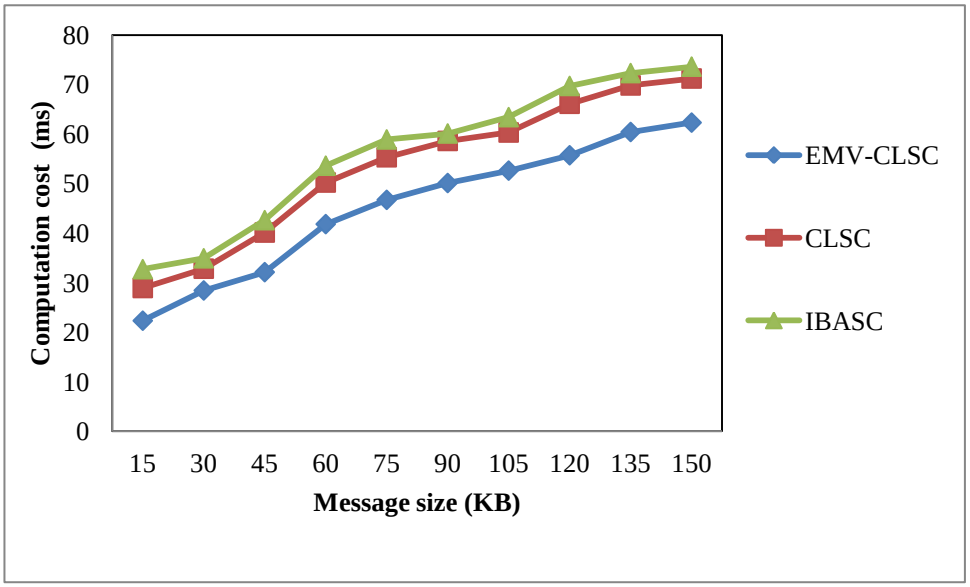

Figure 4 Measure of Computation Cost

Figure 4 clearly describes the computation cost based on the different message size in KB. From the figure, it is clearly illustrates the computation cost of the proposed EMV-CLSC technique is reduced than the state-of-the-art methods [1] [2]. This helps to shows that the proposed EMV-CLSC technique effectively runs a certificate less syncryption algorithm with minimum time. This helps to shows that the efficiency of the proposed EMV-CLSC technique mainly with two aspects signcrypt and verifies the operations. The proposed EMV-CLSC technique provably increases the network security with public key verifiability. Based on, the authorized users only access the message and avoid the unauthorized user in mobile network. Therefore this process takes minimum amount of time to distribute the multiple messages concurrently with a secured manner. The computation cost of the proposed EMV-CLSC technique is reduced by 19% and 26% compared to existing CLSC [1] and IBASC [1] respectively.

5.2 Impact of Memory consumption

Memory consumption is the difference between the total memory for storing the multiple messages and the unused memory. The mathematical formulation of memory consumption is as given below,

$$MC = Total\ memory\ for\ storing\ the\ multiple\ messages - unused\ memory \quad (8)$$

From (8), the memory consumption'MC' is measured in terms of megabytes (MB). Lower the memory consumption more efficient the method is said to be.

Table 3 Tabulation for Memory consumption

Message size (KB)	Memory consumption (MB)		
	EMV-CLSC	CLSC	IBASC
15	132	148	172
30	147	155	190
45	159	178	210
60	201	220	239
75	210	235	251
90	220	247	282
105	243	260	300
120	262	280	310
135	284	296	321
150	293	312	345

As listed in table 3, the amount of memory utilized to store the multiple messages with different size. The memory consumption of the proposed EMV-CLSC technique with respect to different number of message size is varied accordingly. It is measured in terms of Mega Bytes (MB). The memory consumption for the multiple data communication is reduced in proposed EMV-CLSC technique than the state-of-the-art methods.

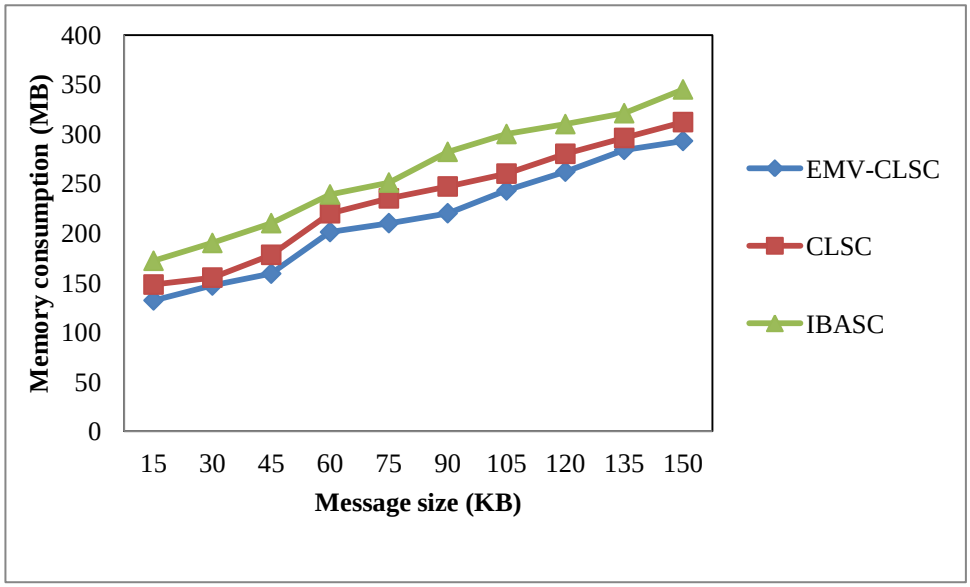

Figure 5 Measure of memory consumption

Figure 5 clearly describes the memory consumption with respect to different number of message size. The result provided in figure 5 confirms that the proposed EMV-CLSC technique significantly outperforms than the other two existing methods CLSC [1] and IBASC [1]. The memory consumption is reduced in the EMV-CLSC technique using the certificateless signcryption algorithm. With the application of certificate less sign cryption algorithm, the different input messages are encrypted with certificate less environment when writing onto the memory. Therefore, the proposed EMV-CLSC technique utilizes less memory consumption for processing the multiple data. In addition, the multilinear vectorized model handles multiple data format while distributing the message simultaneously. This in turn reduces the amount of memory utilization while processing the multiple data. Therefore, the memory consumption is reduced by 9% and 23% compared to existing CLSC [1] and IBASC [1].

5.3 Impact of Communication overhead

Communication overhead is defined as the amount of time required to secure multiple message distribution between senders and receiver. The communication overhead is defined as follows,

$$CO = No.of\ messages * Time\ (\ secured\ message\ distribution) \quad (9)$$

From (4), Communication overhead (CO) is the time taken to multiple message distribution and it is measured in terms of milli seconds (ms). Lower the communication overhead, more efficient the method is said to be.

Table 4 Tabulation Communication overhead

No. of message sent	Communication overhead (ms)		
	EMV-CLSC	CLSC	IBASC
5	12.7	16.2	18.2
10	14.6	18.6	22.3
15	18.3	20.8	24.5
20	22.8	26.3	30.5
25	23.4	30.2	32.9
30	28.2	35.6	40.2
35	31.5	38.1	41.3
40	32.9	41.2	42.5
45	33.8	42.5	44.7
50	37.5	45.8	50.3

Table 4 illustrates the communication overhead during the multiple message distribution based on three different methods EMV-CLSC technique, Certificate Less Sign Cryption (CLSC) [1] and identity-based aggregate Sign Cryption scheme (IBASC) [2]. The proposed EMV-CLSC technique reduces the communication overhead than the existing methods.hgfe21

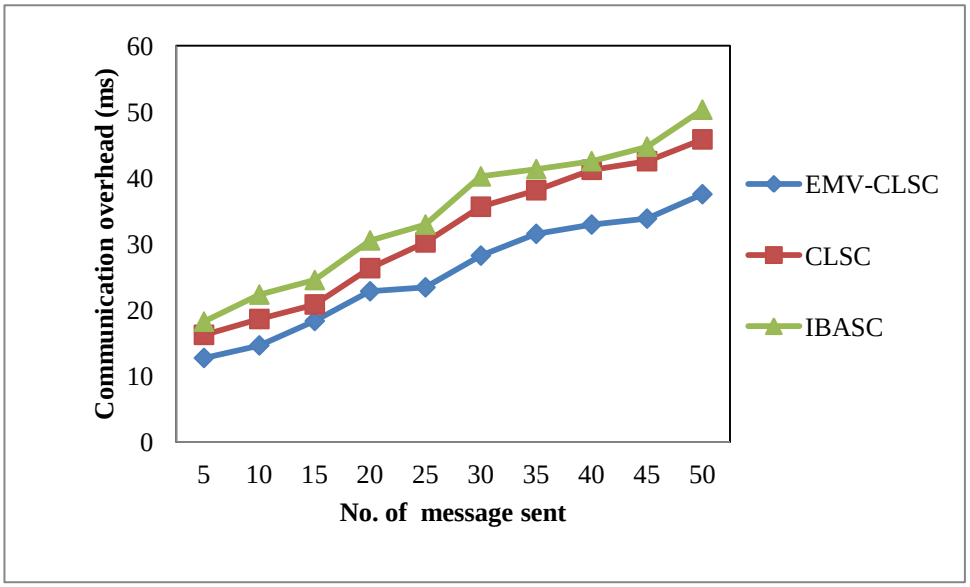

Figure 6 Measure of communication overhead

Figure 6 clearly illustrates that the measurement of communication overhead with different number of message being sent. The simulation performance result clearly reveals that the proposed EMV-CLSC technique utilizes the minimum time to distribute the message from sender to receiver in a secured manner than the other methods [1] [2]. Due to increasing the network transmission range, the several unauthorized user involving for multiple message communication between the senders to receiver. So in order to overcome the problems in secured data transmission with minimum time, the EMV-CLSC technique is proposed. The proposed EMV-CLSC technique uses the sign cryption procedure which utilizes the private key, secret key and public key of the sender based on the certificate less environment. The identity based encryption is used to convert the original message in cipher text. This cipher text is used as a input of the receiver. The cipher text is converted into plain text with the help of private key of the receiver. Therefore, the proposed EMV-CLSC technique improves the secured message communication between senders to receiver with minimum overhead. In addition, the multiple messages are handles by the vector zed model reduces the communication overhead by 23% and 37% compared to existing CLSC [1] and IBASC [2] respectively.

5.4 Impact of Secured message distributing rate

Secured Message distributing rate is the ratio of number of message received at the receiver to the messages being sent and it is measured in terms of percentage (%). The formula for secure message distributing rate is given as below,

$$SMDR = \frac{No.of\ messages\ received}{No.of\ messages\ sent} * 100 \qquad (10)$$

From (10), where $SMFR$ is the Secured message distributing rate.

Table 5 Tabulation for Secured message distributing rate

No. of message sent	Secured message distributing rate (%)		
	EMV-CLSC	CLSC	IBASC
5	78.52	65.36	63.25
10	80.12	68.15	65.31
15	83.65	70.10	67.85
20	85.10	72.52	69.65
25	86.65	74.68	70.54
30	88.36	78.65	73.52
35	90.10	80.10	76.85
40	91.65	82.45	79.65
45	93.32	84.65	82.10
50	95.10	86.65	83.36

Table 5 clearly describes that the secured message distributing rate measurement based on three different techniques. For the simulation analysis, the number of message is varied from 5 to 50. The result reveals that the proposed EMV-CLSC technique increases the secured message broadcasting rate than the existing Certificate Less Sign Cryption (CLSC) [1] and identity-based aggregate signcryption scheme (IBASC) [2].

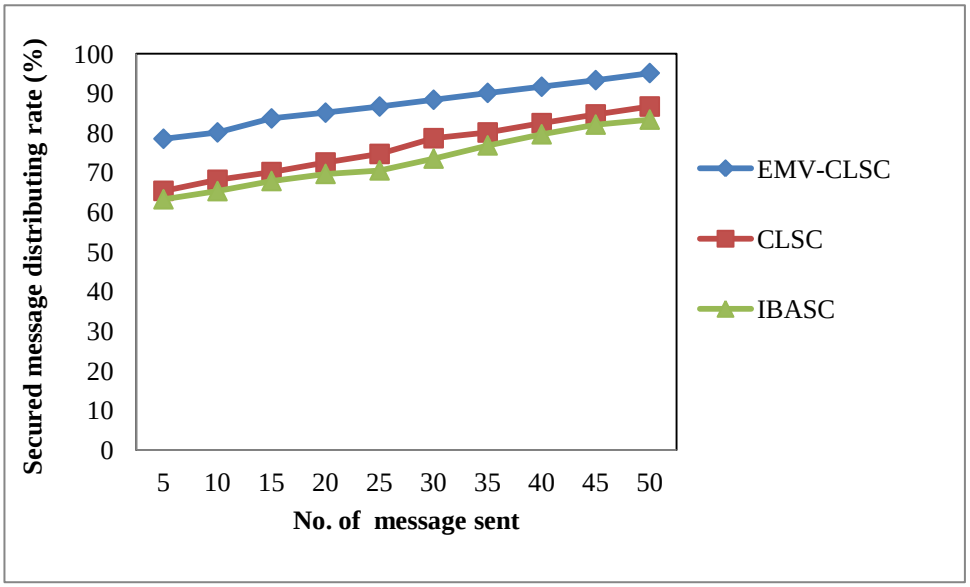

Figure 7. Measure of Secured Massage Broadcasting Rate

Figure 7 clearly illustrates that the secured massage broadcasting rate with different number of messages sent at the range of 5 to 50 with varying sizes at different simulation periods using NS2. From the figure, the number of message being sent is increased the message forwarding rate also gets increased in all methods. But comparatively the proposed EMV-CLSC technique increased the secured massage broadcasting rate. This is because; the certificate less sign cryption process is applied to convert the plain text into cipher text for distributing the message from sender to receiver end with the help of secret key and public key generation. In addition, the Digital Signature verification is performed in proposed EMV-CLSC technique using if-then condition. If the condition is satisfied, the signature is valid or else the signature is invalid. This helps to further enhance the security of message distributing rate using EMV-CLSC technique and also improving the mobile network security. Therefore, the secured message distributing rate is increased by 13% and 16% compared to existing CLSC [1] and IBASC [2] respectively.

6. CONCLUSION

An efficient technique called as Exponentiated Multilinear Vectorized Certificateless Signcryption (EMV-CLSC) is introduced to improve the secured message communication in mobile networks. The proposed EMV-CLSC technique performs the multiple messages broadcasting with minimum communication overhead. The user in certificate less environment performs the signcryption with private and public of the sender and receiver. The signcryption is a public-key cryptography that simultaneously performs the functions of both encryption and digital signature. The Encryption is the most efficient approach to read an encrypted file and converted the plain text into cipher text with the help of secret key. After that, the digital signature is verified with the public key of sender and the unsyncrption is performed with the private key of receiver for generating the secret key. This helps to ensure the mobile network security. In addition, the multilinear vectorized model is used in EMV-CLSC technique for handling the multiple data format in order to reduce the memory consumption. A single syncrption operation with multiple bits is used to highly secure the broadcasted message in EMV-CLSC technique. The simulation is carried out for different parameters such as computation cost, Memory consumption, Communication overhead and Secured message distributing rate. The performance results show that the EMV-CLSC technique improves the secured message distributing rate in terms of less memory consumption, minimum communication overhead and computation cost than the state-of-art methods.

7. REFERENCES

[1] Fagen Li, and Jiaojiao Hong, “Efficient Certificateless Access Control for Wireless Body Area Networks”, IEEE Sensors Journal, Volume 16, Issue 13, July 2016, Pages 5389- 5396

[2] Han Yiliang and Chen Fei, “The Multilinear maps based Certificateless Aggregate Signcryption Scheme”, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2015, Pages 92 - 99

[3] Hasen Nicanfar, Paria Jokar, Konstantin Beznosov, and Victor C. M. Leung, “Efficient Authentication and Key Management Mechanisms for Smart Grid Communications”, IEEE Systems Journal, Volume 8, Issue 2, June 2014, Pages 629 – 640

[4] Yi-Pin Liao , Chih-Ming Hsiao, “A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol”, Ad Hoc Networks, Elsevier, Volume 18, July 2014, Pages 133–146

[5] Ye Tian, Yanbin Peng,Xinguang Peng, and Hongbin Li, “An Attribute-Based Encryption Scheme with Revocation for Fine-Grained Access Control in Wireless Body Area Networks”, International Journal of Distributed Sensor Networks, Hindawi Publishing Corporation, Volume 2014, November 2014, Pages 1-9

[6] Nai-Wei Lo and Jia-Lun Tsai, “A Provably Secure Proxy Signcryption Scheme Using Bilinear Pairings”, Journal of Applied Mathematics, Hindawi Publishing Corporation, Volume 2014, pages 1-10

[7] Rawya Rizk, Yasmin Alkady, “Two-phase hybrid cryptography algorithm for wireless sensor networks”, Journal of Electrical Systems and Information Technology, volume 2, 2015, Pages 296–313

[8] Chunqiang Hu, Nan Zhang, Hongjuan Li, Xiuzhen Cheng, and Xiaofeng Liao, "Body area network security: a fuzzy attribute-based signcryption scheme", IEEE Journal on Selected Areas in Communications/Supplement, Volume 31, Issue 9, 2013, Pages 37–45

[9] S.Padma, D.C. Joy Winnie Wise, S. Malaiarasan, N. Rajapriya, "Ensuring Authenticity and Revocability for Wireless Body Area Network using Certificateless Cryptography", International Research Journal of Engineering and Technology (IRJET), Volume 03 Issue 03, March 2016, Pages 171-1715,

[10] Kanaga Suba Raja, Usha Kiruthika, "An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV", Wireless Personal Communications, Springer, Volume 83, Issue 4, 2015, Pages 2975–2997,

[11] Madhumita Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research (AJER), Volume 03, Issue 01, 2014, Pages 50-56

[12] Zhongyuan Qin, Xinshuai Zhang, Kerong Feng, Qunfang Zhang, and Jie Huang," An Efficient Key Management Scheme Based on ECC and AVL Tree for Large Scale Wireless Sensor Networks", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Volume 2015, August 2015, Pages 1- 7

[13] Krishna Kumar Pandey, Vikas Rangari, Sitesh KumarSinha, "An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security", International Journal of Computer Applications, Volume 74, Issue 20, July 2013, Pages 0975 – 8887

[14] Yang Lu and Jiguo Li, "Efficient Certificate-Based Signcryption Secure against PublicKey Replacement Attacks and Insider Attacks", the Scientific World Journal, Hindawi Publishing Corporation, Volume 2014, May 2014, Pages 1-12

[15] Shyam Nandan Kumar, "Review on Network Security and Cryptography", International Transaction of Electrical and Computer Engineers System, Volume 3, Issue 1, 2015, Pages 1-11

[16] SK Hafizul Islam and G.P. Biswas, "Certificateless short sequential and broadcast multi signature schemes using elliptic curve bilinear pairings", Journal of King Saud University – Computer and Information Sciences, Elsevier, Volume 26, 2014, Pages 89–97

[17] Charru, Paramjeet Singh, Shaveta Rani, "Improved Cryptography Algorithm to Enhanced Data Security", International Journal For Research in Applied Science and engineering technology (IJRASET) , Volume 2, Issue IX, September 2014, Pages 242-247

[18] Madhusanka Liyanage ,Ahmed Bux Abro ,Mika Ylianttila and Andrei Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security", IEEE Security & Privacy, Volume 14, Issue 4, 2016, Pages 34 – 44.

[19] Wei Liu , Hiroki Nishiyama, Nirwan Ansari , Jie Yang , Nei Kato, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Transactions on Parallel and Distributed Systems , Volume 24, Issue 2, February 2013, Pages 239 – 249

[20] Jian Shen, Haowen Tan, Sangman Moh, Ilyong Chung, Qi Liu, and Xingming Sun, "Enhanced Secure Sensor Association and Key Management in Wireless Body Area Networks", Journal Of Communications And Networks, Volume 17, Issue 5, October 2015, Pages 453-462.