Efficient Modified Elliptic Curve Diffie-Hellman Algorithm for VoIP Networks

Subashri Thangavelu[1] and Vaidehi Vijaykumar[2]
[1]Department of Electronics Engineering, Anna University, India
[2]AU-KBC Research Centre, Anna University, India

Abstract: *Security in Voice over Internet Protocol (VoIP) network has turned to be the most challenging issue in recent years. VoIP packets are easy to eavesdrop on by hackers due to the use of Diffie-Hellman (DH) algorithm for single common key exchange between two end-users. As a result the confidentiality of voice data turns to be a challenging issue. There is a need for strong key management algorithm to secure voice data from all kinds of attacks. In this paper, an efficient Modified Elliptic Curve Diffie-Hellman (MECDH) using Split Scalar Multiplication (SSM) algorithm is proposed, which secures voice data from Man-in-the Middle (MITM) attack by dynamically generating the shared key. Further, in order to speed up the Scalar Multiplication (SM) used in traditional Elliptic Curve Diffie Hellman (ECDH) algorithm, the SSM technique is adopted in the proposed MECDH algorithm. The performance of the proposed MECDH algorithm is compared with the traditional ECDH and validated in Java platform. From the results obtained, it is observed that the computation time taken by the proposed MECDH algorithm is 89% lesser than the traditional ECDH algorithm and 11% lesser than the key changing ECDH. Also, high security level is achieved with the proposed idea of using dynamic keys instead of single common shared secret key.*

Keywords: *Elliptic curve, key exchange, key change, MITM attack, SSM, computation time.*

Received March 5, 2013; accepted May 10, 2014; published online October 29, 2015

1. Introduction

Voice Over Internet Protocol (VOIP) has experienced tremendous growth from the recent years because of its low cost and its capability of rendering new services. It is a technology that allows users to make telephone calls using a broadband internet connection instead of an analog phone line. However, compared with traditional telephone systems, it is more vulnerable to security attacks. Also, VoIP faces degradation, security attacks due to its operation on the public internet [13, 30].

An efficient encryption algorithm for voice data encryption with the less number of computations would be the best solution to overcome the attacks related to the confidentiality services of VoIP data [1, 21]. Advanced Encryption Standard (AES) is more suitable [25] as it involves the values of speed and security to provide secured end to end VoIP services. Since, AES is a symmetric key cryptosystem, it requires key exchange algorithm like traditional Diffie-Hellman (DH) algorithm to negotiate a common shared secrete key without the need of key distribution center [11, 26, 28]. The inverse nature of exponentiation and logarithm of conventional DH algorithm allows hacker to lacerate the generated single common shared secret key. The Modular Exponentiation (ME) in key generation allows an attacker to use Discrete Logarithm (DL) for hacking the generated single common shared secret key. Consequently, it is susceptible to DLP attack, the secrecy of key exchange can be preserved based on solving the Discrete Logarithm Problem (DLP) [4, 9, 26].

Another version of DH which is used for VoIP data confidentiality is the Key Changing DH (KC-DH) [34]. This solution is ended with multiple dynamic key negotiated with the help of dynamic key updating process for the generated single common shared secret key during the same VoIP call period. Man-in-the-Middle (MITM) attack is also prevented by the secret way of shared key exchange. Hence, it allows hackers to retrieve the generated shared key because of the inverse property of ME and DL in the traditional DH algorithm. The secrecy of the key exchange by KC-DH is based on the difficult part of DLP [7, 26].

Another solution for key exchange in an end to end call set up is Elliptic Curve Diffie Hellman algorithm (ECDH) [16, 17, 31]. It is found to be one of the promising solutions for the key exchange mechanism in VoIP call signalling, in which the negotiated common shared secret key is used to encrypt voice data from both the parties to protect the voice data from the MITM attack [2, 13]. It is an attractive alternative for traditional DH algorithm because of the minimum computations on the elliptic curve arithmetic operations rather than the complex DL operations over the DH algorithm. The attributes of key generation by elliptic curve group in ECDH algorithm makes the DLP into more difficult Elliptic Curve Discrete Logarithm (ECDLP) for hacker. The secrecy of ECDH is now based on the difficult part of ECDLP [7, 16, 35].

The adoption of elliptic curve schemes in the key exchange algorithm can minimize the computational load, which is an added advantage for the key

exchange mechanism for VoIP applications. But the security level of the key is maintained as the same even with the smaller key size than the existing algorithms [31, 35]. However, this ECDLP is addressed in the Pollard Rho (PR) and Polling Hellman (PH) factorization methods [35] and the hacker is allowed to make the ECDLP attack to retrieve the generated shared secret key. So, the secrecy of the generated shared secret key by ECDH algorithm is not secret any more [7, 35]. Hence, there is a need for changing the key dynamically which is generated by ECDH algorithm during the VoIP call set up.

This work presents an approach to constrict the secrecy of key generation process by dynamically changing the generated shared secret key of the ECDH algorithm. A modified key altering function is included in the final step of the ECDH key generation procedure for randomizing the key. Hence, ECDH algorithm is called as Modified ECDH (MECDH). The random nature of shared secret key provides good quality data encryption solution for maintaining the confidentiality of VoIP data.

The required randomized shared secret key for the current packet encryption is generated by iteratively invoking the key altering function. The sequence number in the Real Time Transport (RTP) packet gives the number of iterations to be performed by the key altering function. The time for generating the updated key is very less because of simple computation in the key update process. The update process depends only on the initially received constants from RTP packets.

In spite of dynamically altering the generated shared secret key in MECDH algorithm, the Scalar Multiplication (SM) increases the VoIP packet delay, computational complexity and execution time. In this paper, Split Scalar Multiplication (SSM) [10] is adopted for dynamic key generation process which reduces the computations involved in scalar multiplication. Thus, the adopted technique improves the performance of the MECDH. The paper is organized as follows: Section 2 discusses the related work in VOIP and security mechanisms in key management process. The proposed work is described in section 3. The validation and evaluation of the proposed work is presented in section 4. Section 5 concludes the paper.

2. Related Works

Current research in VoIP network focuses on enforcing security and providing quality of service in VOIP [1, 21]. Among these issues, confidentiality of voice packet turns to be a challenging task [2, 8, 13, 19]. The voice packet transmission over the public internet using the transparent IP protocol suite makes the confidentiality of the voice data at risk because of the inefficient key exchange protocols in VoIP environment [2].

The key exchange process for media encryption faces different kinds of attacks [1, 2, 3, 4, 13]. Strong key management protocols are needed for secured voice data packet transmission that includes key exchange of establishment protocols. A shared secret-key exchange between communicating parties is termed as key establishment protocol [7, 16, 24, 37]. It is used to communicate securely between end users over an open network [1, 4, 6, 7]. The conventional key exchange algorithms such as DH in Zimmermann Real Time Transport Protocol (ZRTP), Session Description Protocol (SDP) [14] Security Descriptions (SDES) and Multimedia Internet Keying (MIKEY) [2] of VoIP key exchange protocols use a single common shared secret key between two communicating parties [1, 2, 6, 15]. There is a need for extending the key exchange protocols of VoIP network to prevent MITM attack over the public internet environment. An efficient key exchange protocol with high security level is achieved through dynamic key [1, 4, 34].

The dynamic function of the conventional DH also, influences the MITM attack for the initial key exchange process and subside the entire procedure. The most secret way of initial key exchange process is expected for a highly secured environment. The secrecy of the key exchange process is preserved by the Elliptic Curve Cryptography (ECC) because of the points of the elliptic curve group is regenerated only by the elliptic curve shared users. Elliptic curve based DH key exchange is the best alternative for key exchange process where the secrecy of the process is high rather than the conventional DH. The factorization method of elliptic curve that retrieves the points of elliptic curve group allows the hacker to intrude. Hence, the proposed key altering function for secret key exchange method overcomes the problem posed by factorization methods.

Another ECC based security mechanism named enhanced Session Initiation Protocol (SIP) authentication scheme is suggested by Pu and Wu [27] for authenticating SIP user. The enhanced SIP authentication scheme prevents off-line password guessing attacks by the ECC. The experimental analysis proved that the enhanced SIP authentication scheme based on ECC has improved security level than the existing SIP authentication schemes. Security analyses against different attacks have been done and performance results showed that it prevents stolen verifier attack and password guessing attack.

ECC based security schemes such as authentication and confidentiality security services are suggested for SIP protocol [36]. The adoption of elliptic curve schemes in security services consume computation time based on the number of elliptic curve point multiplication. Therefore, using ECC based authentication and confidentiality schemes consume much time for computation in real time VoIP application. The authors have not discussed the computational complexity of ECC authentication and confidentiality service for SIP protocol [27].

Ismail [20] presented an architectural solution for implementing VoIP over Virtual Private Network (VPN). Their experimental analysis concluded that the VoIP over VPN through hardware device provides

better performance compared to the performance of VoIP over VPN with open source application. Also, they have mentioned the role of technique in improving the quality of VoIP over VPN using mesh wireless network.

Subramaniam and Kuppuswami [32] also, presented the performance of DH key agreement protocol on several of ECC based enhanced security mechanisms between E-passport and examination system. The authors have generated the secured session key using DH key agreement protocol with ECC by biometric values which suits real time applications. But, the author has failed in measuring the performance of the key agreement protocol in real time environment [32].

2.1. DH Algorithm

2.1.1. The Conventional Algorithm

Diffie and Hellman [11] proposed an algorithm for key exchange process. The secrecy of this algorithm is based on the computation of the DLs. The factorization methods like index calculus methods are able to split the conventional DH into known parts for hackers [4, 31, 34]. Table 1 shows computational complexity of the various key exchange algorithms. The complexity of the DH is greater than ECDH algorithm.

Table 1. Comparison of computational complexity of key exchanging algorithms.

Sl. No	Algorithm	Computational Complexity
1	DH	O (exp(1.923(log n)1/3(log log n)2/3))
2	Strong DH	O (exp(1.923(log n)1/3(log log n)2/3))
3	KC-DH	O (exp(1.923(log n)1/3(log log n)2/3))
4	ECDH	(√n) where n is the size of bits used in key

2.1.2. The Dynamic DH

The secrecy of the generated single common shared secret key can decide the secrecy of user's information. The negotiated common single key solution is vulnerable to more attacks. An alternative solution to this single common shared secret key is dynamic key generation which involves generating different encryption key for the same pair of users participating in the session. The dynamic key based encryption proves to be efficient for real time applications such as VoIP applications. Also, there is no need of renegotiation of new keys in the DH based dynamic function [34].

The secrecy of the key exchange process also depends on the secrecy of the DH algorithm. The dynamic keys generated by DH algorithm are possibly be attacked by hackers, because the MITM attack is based on the same initial seed that was used to derive the entire dynamic common shared secret key. Therefore, the dynamic key function is not effective for VOIP application. Hence, there is a need for designing a strong and dynamic key exchange algorithm that enables secured shared secret key exchange [17, 34].

2.1.3. ECDH Algorithm (ECC)

ECC is one of the public key cryptography methods. Most of the public key algorithms expect the devices which are participating in the communication to know a set of already defined constants [17]. The domain parameters used in the ECC is an example of such constants. The mathematical operations of the ECC [17, 18] is defined over the elliptic curve.

$$y^2 = x^3 + ax + b \quad (1)$$

Where

$$4a^3 + 27b^2 \neq 0 \quad (2)$$

2.1.4. ECDH

Elliptic curve functions in key generation combined with exchange procedure for shared secret key preserves the secrecy. In the public key cryptography, each user uses a pair of keys, i.e., public and the private keys at each end of communicating part. Only the specific user knows the private key whereas the public key is distributed to all users. The public key is a point on the elliptic curve and the private key is from some random number [17]. Shared secret key is generated using private and public keys. Hence, all the users can take part in the communication using the shared secret key.

An multiplication of a random number 'G' from an algebraic group integer set by an elliptic curve points in the elliptic curve algebraic group have produced the public key by the SM property of elliptic curve arithmetic [17]. The SM of the elliptic curve points by an integer scalar is the dominating operation in elliptic curve function of key exchange algorithm [4, 34]. Though the elliptic curve function has increased the secrecy of the key exchange algorithm in ECDH, the number of arithmetic operation decides the computational complexity of the algorithm [5, 34]. A number of fast SM algorithms have been proposed in literature [5] to improve the performance of elliptic curve scalar multiplications in ECC.

Further, the computational complexity of the SM can be reduced by adopting the SSM [10]. In this paper, SSM in elliptic curve functions of ECDH algorithm is used to reduce the computational complexity. The major advantage of adopting elliptic curve function in key generation functions is its smaller key size for encryption [18, 31]. Another advantage of the ECDH is the secured exchange key procedure using shared secret key generation [31, 34]. Table 2 shows the NIST guidelines to select the key for AES algorithm.

Table 2. NIST Guidelines for using AES keys.

ECC Key Size (bits)	RSA/DH Key Size (bits)	Key Size Ratio ECC Vs RSA/DH	AES Key Size (bits)
163	1024	1:6	128
256	3072	1:12	128
384	7680	1:20	192
512	15360	1:30	256

2.1.4.1. Limitations on ECDH

The DLP of the traditional DH key exchange algorithm has become ECDLP in ECDH algorithm. The elliptic curve parameters for the cryptographic scheme should be carefully chosen in order to resist all the known attacks on the ECDLP. The hardness of the ECDL is essential for the security of the ECDH. PR factorization method and other current factorization methods are used for factoring the curve modular logarithms [16] of the ECDH algorithm.

Another challenge in the key distribution protocol is the efficiency of the algorithm, which depends on the number of computations [4, 12, 23, 31]. The exponent operations including ME and SM on an elliptic curve is the most primitive operation which is dominating the computation time. To reduce the time complexity of key distribution algorithm, the idea of using SSM instead of SM is put forth in this paper.

2.2. VoIP Key Exchange Protocols

Figure 1 illustrates the basic VoIP network architecture consisting of end user equipment, a gateway, and other network components. The encryption of VoIP voice data requires the key negotiation through common signalling protocols of VoIP network in prior. VoIP signalling protocols play a major role in VoIP call set up procedures [1, 8, 19, 29, 30]. A number of application layer based signalling protocols such as conventional H.323, SIP, SDP exist for VoIP call initiation process which is similar to the internet signalling protocol [22, 29]. The packet of SIP signalling protocol consists of the start-line, message header and body of messages.

The start-line of the SIP message consists of the request and response messages of SIP message. The SIP signalling of request and response completes the operation of VoIP session for voice communication. The key exchange information is negotiated using the SDP which is a SIP companion protocol [2, 14, 29]. The information about the negotiated key by DH is exchanged between the end users with the help of the SIP request and responses. Thus, the SDP protocol provides synchronization between two ends of users. In SDP packet, the option k carries the public keys of DH participating in the negotiation of common shared secret key for calling parties [19].

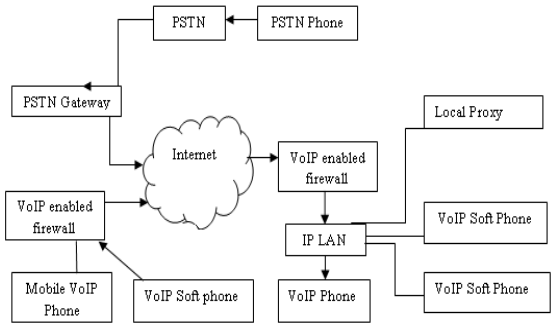


Figure 1. VoIP Architecture.

After successfully completing the call set up procedure by SIP, the RTP carries either the raw or encrypted payload of voice data. This protocol operates on the UDP of the transport-layer protocol to support the real time multimedia applications. The function of the RTP protocol is packet loss detection and synchronization of media play back between end users [33].

In DH, the exponential arithmetic process which is time consuming is not suitable for low power mobile based VoIP applications. This process may delay VoIP call set up procedure. The exponential arithmetic can be changed into additive arithmetic of ECDH with simple computations by ECC [5, 10]. The ECC has faster computing time and smaller storage; therefore it is suitable for ubiquitous computing devices [18, 31, 32].

Figure 2 shows the complete connection set up process in VoIP communication using SIP and RTP protocol. The session establishment and control are taken care by the SIP signalling protocol. The RTP protocol transfers the VoIP payload during the VoIP communication.

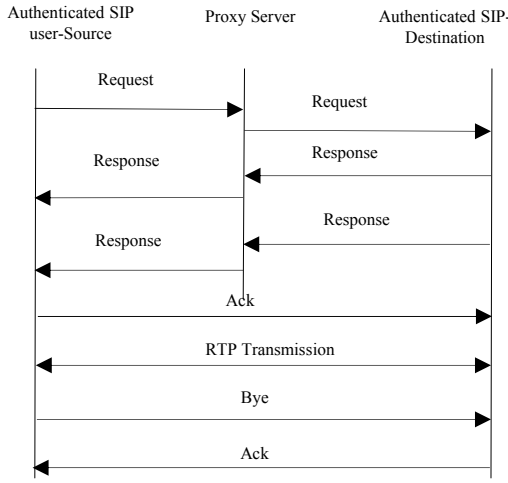


Figure 2. VoIP signalling messages using SIP message.

3. The Proposed MECDH Algorithm

The protocols for VoIP key exchange process need to be immune for MITM attack by some detecting and secured algorithm [1]. The dynamic key is a solution which is proposed in [34] to update the VoIP key dynamically. The conventional DH is used for the key generation, which is vulnerable to MITM attacks. In VoIP, the development of the key exchange protocols for VoIP is not much focused and efficient key management protocol is much essential. The research on speeding up another exponentiation operation in DL based algorithms strives to reduce the total number of complex components as well as the complexity of the individual operations.

3.1. The Proposed MECDH Algorithm using SSM

In this paper, efficient Modified Elliptic Curve Diffie Hellman (MECDH) is proposed to provide dynamic

key for VoIP data confidentiality. The efficiency of the protocol is improved by reducing the number of point multiplication on elliptic curves using SSM [10]. The proposed efficient MECDH includes two levels of improvements over the elliptic curve key agreement protocol.

The encryption key is changed frequently during a VoIP call session. The two end users are immediately identified, and the keys are updated for voice packets encryption without any new SIP update message which causes for traffic load. This improves the level of security of the key agreement algorithm. Next one is the computation reduction function is performed based on the SSM [10] on the key changing function.

Figure 3 shows the steps involved in exchanging the parameters for generating the public key and exchanging the public key for producing shared secret key. The generated shared secret key is used to encrypt the VoIP packet payload and the RTP protocol carries the encrypted payload to other end.

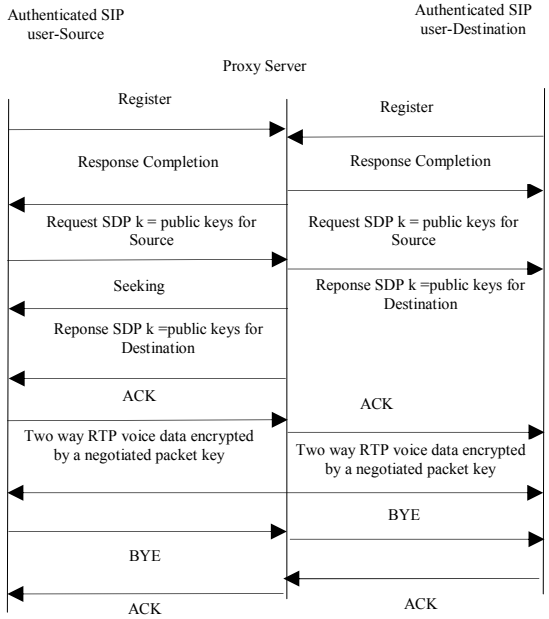
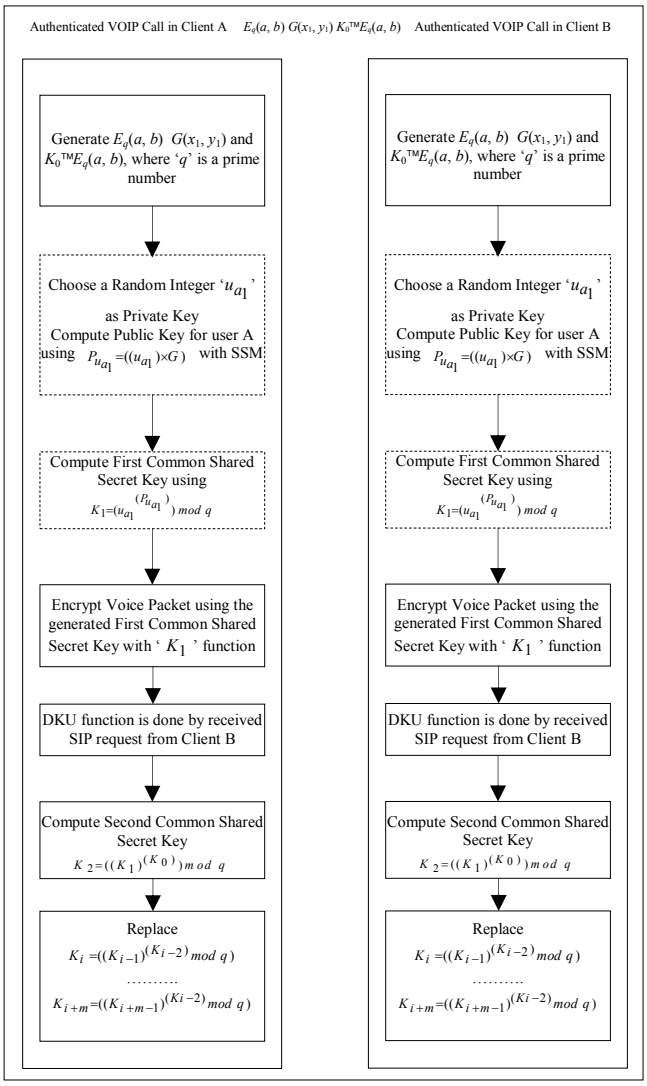


Figure 3. The exchange of parameters of shared secret key generating algorithm in SIP VoIP network.

Figure 4 shows the header details in VoIP packet. Figure 5 shows the proposed efficient MECDH algorithm for shared secret key generation process. The dotted boxes indicate the adopted SSM for SM process in public key generation of DH algorithm. The common shared secret key is generated by the shared secret key generating function using the received public key. The exponential arithmetic operations of common shared secret key generation have been reduced considerably by proposing a modified common shared secret key generating function in MECDH algorithm. The initial common shared key is updated by the dynamic key update (DKU) function during the same VoIP session.

IP Header (20 bytes)	UDP Header (8 bytes)	RTP Header (12 bytes)	Sequence No	RTP Payload of Encrypted voice packet (20 to 160 bytes)

Figure 4. Header details in VoIP packets.



* RTP Transmission

** No need of update message in SIP to change key

Figure 5. The MECDH algorithm in SIP message during VoIP call communication.

In order to increase the privacy protection of VoIP call session from using single common shared secret key for voice data encryption, the dynamic key [10] based encryption of voice via MECDH without having any disturbance of voice quality has been proposed. The proposed MECDH is applied in SIP signalling to update the shared secret key during the VoIP call session.

The proposed Efficient Elliptic Curve DH algorithm using the fast SSM [11] is shown in Algorithm 1.

Algorithm 1: The Proposed dynamic key generation using MECDH with SSM.

Begin

Generate $E_q(a, b)\ G(x_1, y_1)$ *and* $K_0 \text{™} E_q(a, b)$, *where 'q' is a prime number.*

Choose Random Number $u_{a1} \text{™} E_q(a, b)$ *as a Private Key of Client A.*

Calculate public key $P_{u_{a_1}}=((u_{a_1})\times G)$, *Where G is* $\text{™} G(x_1, y_1)$. *SM in public key generation is replaced by SSM.*

Calculate common shared secret key $K_1=((u_{a_1})^{(P_{u_{a_1}})} \bmod q)$. *SM in product of value* $(u_{a_1}\times P_{u_{a_1}})$ *is replaced by SSM.*

Algorithm 2.

Single common shared secret key is generated using proposed SSM.
Now, voice packets are encrypted using by AES encryption algorithm with generated Single Common Shared Secret Key.
DKU is adopted for generating dynamic keys in SIP request.
Update the shared secret key using

$k_{i-1} = (k_{i-2})^{(k_{i-3})} \bmod q, k_i = (k_{i-2})^{(k_{i-1})} \bmod q, \ldots,$

$k_2 = (k_1)^{(k_0)} \bmod q$

End

Algorithm 2: SSM method algorithm.

Input P, Q, k_1, k_2

Scanning Stage

1. $R_i = 0$ *and* $i = 0, 3, 5, \ldots, (2^{w-1}-1)$
2. *For* j-0 *to* $(m$-1)

$$Set\ R_{\left|k_{1,j}\right|} \rightarrow R_{\left|k_{1,j}\right|} + sign(k_{1,j}) \times (\tau_j(P))$$

$$Set\ R_{\left|k_{1,j}\right|} \rightarrow R_{\left|k_{1,j}\right|} + sign(k_{1,j}) \times (\tau_j(P))$$

3. $Compute\ ((k_1 \times P) + (k_2 \times Q)) = (R_1 + 3 \times R_3 + \ldots (2^{(w-1)} - 1) \times R^{2w-1} - 1)$

   a. $Set\ S \rightarrow (R^{2^{w-1}} - 1)$ *and* $T \rightarrow (R^{2^{w-1}} - 1)$

   b. *For* $i = ((2^{w-1} - 3), (2^{w-1} - 3), \ldots, 5, 3, 1)$

      $Set\ S \rightarrow (S + R_i)$

      $Set\ T \rightarrow (T + S)$

4. $Set\ T \rightarrow 2T$
5. $Set\ T \rightarrow T + S + R_i$

Output of SSM.

4. Results and Discussions

The performance of various key exchanging algorithms such as conventional DH, KC-DH, conventional ECDH and MECDH are compared interms of computational complexity and the results are presented in Table 3. Simulation of static and dynamic key generation for secured VOIP is done using Java Jdk 1.7.0 with Netbeans 6.0 as Integrated Development Environment (IDE). The performance of conventional DH, dynamic DH, ECDH and MECDH and the proposed efficient MECDH that uses the SSM methods are evaluated. The observed results show the computation time of the traditional DH time as 1040ms and ECDH as 380ms in Intel R core i-5-2400 CPU with the processor speed of 3.10Ghz.

Table 3. Execution time for various algorithms in voice packet encryption.

Sl. No	Name of the Algorithm	Elliptic Curve Point Generation Algorithms using ECC	Static Key Generation using ECDH Algorithms	Voice packet Encryption using Different SM on ECDH based AES
1	NAF	42	96	519
2	τ NAF	27	83	503
3	ω NAF	20	77	481
4	ω τ NAF	15	71	466
5	SSM Single Key (SSM ECDH)	10	63	141
6	SSM Dynamic Key (SSM MECDH)	10	130	203

For comparing the proposed MECDH algorithm, standard benchmark algorithm such as Non-Adjacent Form (NAF), t-adic Non-Adjacent Form (t-NAF), w-Non-Adjacent Form (w-NAF) and width t-Non-Adjacent Form (w tNAF) have taken for evaluations.

Figure 6 shows the performance results of different fast SM methods for elliptic curve arithmetic. The size of the elliptic curve point chosen for the co-ordinates of elliptic curve is 163bits. Similarly, the performance of the ECDH algorithm with different SM methods is evaluated. The observed results are shown in Figure 7.

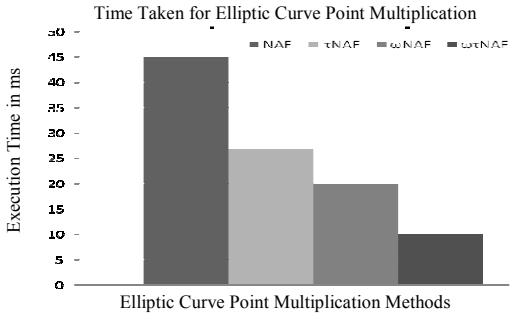


Figure 6. Comparison of fast SM.

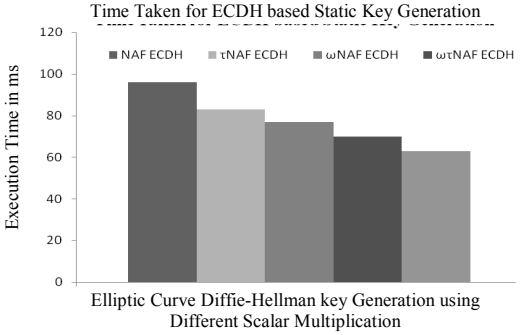


Figure 7. Comparison of fast SM in ECDH.

The encryption of VoIP data using AES based on ECDH key with different SM method is performed and its performance evaluation is shown in Figure 8. Different computations involved in various fast SM methods of ECDH results in varied encryption time for voice packets.

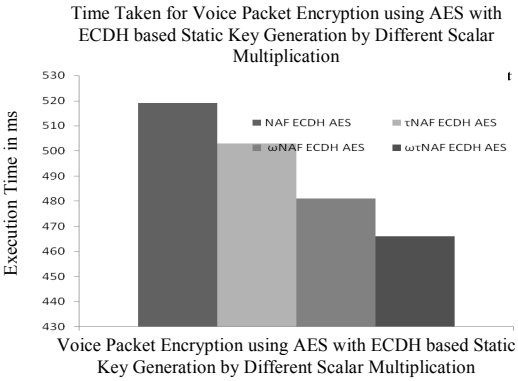


Figure 8. Comparison of fast SM based AES.

Voice packets in VoIP application is encrypted using AES algorithm. The computation time for voice packet encryption is decided by the amount of time required for common shared secret key generation and the amount of time required for encryption process. The high computation time required for encrypting

large size packet using AES based an ECDH key is reduced by adopting different fast scalar multiplications.

The varied encryption time for the large size voice packet is shown in Figure 9 which is done by AES encryption algorithm with different fast SM on ECDH key generation.

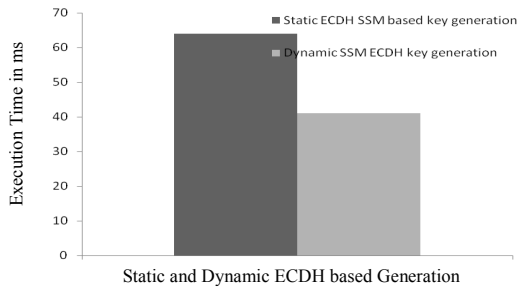


Figure 9. Comparison of fast SM in ECDH.

It is clear that, the SSM based ECDH key generation takes less time rather than ωτNAF based ECDH from Figure 9. The execution time for various algorithms in voice packet encryption is shown in the Table 3. It is observed that the proposed MECDH algorithm takes less time for performing key exchange compared to other existing algorithms.

Figure 10 gives the execution time for NAF SSM based shared secret key generation. The execution time for the generated common shared secret key by NAF SSM based ECDH is 40 ms which is less than 96ms of NAF based ECDH. Figure 11 shows the execution time for NAF SSM based AES result to get encrypted message by the generated common shared secret key. Encryption using NAF SSM based AES is carried out for both sample text and voice packets. Figure 11 shows the performance comparison between the proposed MECDH algorithm and the conventional ECDH with one of the scalar multiplication SSM.

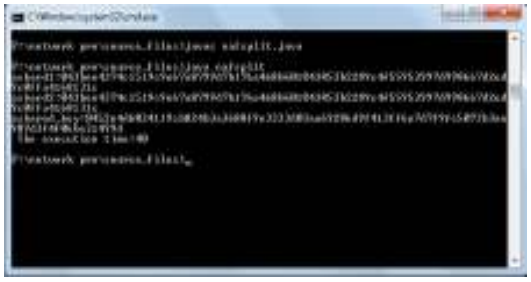


Figure 10. Execution time of the SSM based ECDH key generation in AES encryption for sample text data.

Figure 11. Execution time of the SSM based ECDH key generation in AES encryption for sample VoIP data.

5. Conclusions

New internet technologies like VOIP pose many security problems. It is necessary to prevent eavesdropping in internet applications. The existing key exchanging mechanisms like DH is easily attacked by the hackers using MITM attack and DLP attack. The exchanged key that is used as an initial value for the encryption process reduces the level of security which in turn reduces the strength of an encryption algorithm. To increase the strength of encryption, the existing DH key exchanging mechanism for VoIP packet is replaced by the proposed efficient MECDH in which the dynamic key changing mechanism is proposed to replace the static keys. Also, the computation time involved in efficient MECDH is reduced by 89% using SSM. Hence, proposed efficient MECDH using SSM proves to be more suitable for real time applications like VoIP.

References

[1] Aghila G. and Chandirasekaran D., "An Analysis of VoIP Secure Key Exchange Protocols Against Man-In-Middle Attacks," *the International Journal of Computer Applications*, vol. 34, no. 7, pp. 46-52, 2011.

[2] Arkko J., Carrara E., Lindholm F., Naslund M., and Norrman K., "Multimedia Internet Keying (MIKEY)," *IETF*, RFC 3830, 2004.

[3] Barbieri R., Bruschi D., and Rosti E., "Voice over IP sec Analysis and Solutions," *Proceedings of the 18th Annual Computer Security Applications Conference*, pp. 261-270, 2002.

[4] Barker E., Barker W., Burr W., Polk W., and Smid M., "Recommendation for Key Management: Best Practices for Key Management Organization-Part 2," *NIST Special Publication* 800-57, pp. 1-78, 2007.

[5] Brickell E., Gordon D., McCurley K., and Wilson D., "Fast Exponentiation with Pre Computation: Algorithms and Lower Bounds," available at: https://www.ccrwest.org/gordon/fast.pdf, last visited 1993.

[6] Butcher D., Li X., and Guo J., "Security Challenge and Defense in VOIP Infrastructures," *IEEE Transactions on Systems, Man, and Cybernetics: Applications and Reviews-Part C*, vol. 37, no. 6, pp. 1152-1162, 2007.

[7] Canetti R. and Krawczyk H., "Analysis of Key Exchange Protocols and Their Use for Building Secure Channels," available at: https://eprint.iacr.org/2001/040, last visited 2001.

[8] Cao F. and Malik S., "Vulnerability Analysis and best Practices for Adopting IP Telephony in Critical Infrastructure Sectors," *IEEE Communication Magazine,* vol. 44, no. 4, pp. 138-145, 2006.

[9] Cheon J., "Security Analysis of the Strong Diffie-Hellman Problem," *in Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Russia, pp. 1-11, 2006.

[10] Cheon J., Jarecki S., Kwon T., and Lee M., "Fast Exponentiation Using Split Exponents," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1816-1826, 2011.

[11] Diffie W. and Hellman M., "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[12] Goode B., "Voice over Internet Protocol," *Proceedings of the IEEE*, vol. 90, no. 9, pp. 1495-1517, 2002.

[13] Gupta P. and Shmatikov V., "Security Analysis of Voice-over-IP Protocols," *in Proceedings of the 20th IEEE Computer Security Foundations Symposium*, Venice, pp. 49- 63 2007.

[14] Handley M., Jacobson V., and Perkins C., "SDP: Session Description Protocol," available at: https://tools.ietf.org/html/rfc4566, last visited 2006.

[15] Handley M., Perkins C., and Whelan E., "Session Announcement Protocol," available at: https://tools.ietf.org/html/rfc2974, last visited 2000.

[16] Hankerson D., Hernandez J., and Menezes A., "Software Implementation of Elliptic Curve Cryptography over Binary Fields," *in Proceedings of the 2nd International Workshop on Cryptographic Hardware and Embedded Systems*, *Springer-Verlag*, London, pp. 1-24, 2000.

[17] Hankerson D., Menezes A., and Vanstone S., *Guide to Elliptic Curve Cryptography*, Springer-Verlag New York, 2004.

[18] Hellman M., "An Overview of Public Key Cryptography," *IEEE Communications Society Magazine*, vol. 50, no. 5, pp. 42-49, 2002.

[19] Hung P. and Martin M., "Security Issues in VOIP Applications," *in Proceedings of CCECE'06, Canadian Conference on Electrical and Computer Engineering*, Ottawa, pp. 2361-2364, 2006.

[20] Ismail M., "Study the Best Approach Implementation and Codec Selection for VoIP over Virtual Private Network," *The International Arab Journal of Information Technology*, vol. 10, no. 2, pp. 198-203, 2011.

[21] Kahn R., Walsh J., and Fries S., "Security Considerations for VoIP Systems," available at: http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf, last visited 2005.

[22] Keromytis A., "A Survey of Voice Over IP Security Research," *in Proceeding of the* 5th International Conference, India, pp. 1-17, 2009.

[23] Keromytis A., "Voice-over-IP Security: Research and Practice," *IEEE Secure and Privacy*, vol. 8, no. 2, pp. 76-88, 2010.

[24] Matsumoto T., Takashima Y., and Imai H., "On Seeking Smart Public-Key Distribution Systems," *IEICE Transaction on Information and Communication Theory,* Vol. 69, no. 2, pp. 99-106, 1986.

[25] National Institute of Standards and Technology., "Advanced Encryption Standard," available at http://www.nist.gov/aes, last visited 2001.

[26] National Institute of Standards and Technology., "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)," available at: http://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-56Ar2.pdf, last visited 2007.

[27] Pu Q. and Wu S., "Secure and Efficient SIP Authentication Scheme for Converged VoIP Networks," *The International Arab Journal of Information Technology*, vol. 9, no. 6, pp. 553-561, 2012.

[28] Rescorla E., "Diffie–Hellman Key Agreement Method," available at: https://www.ietf.org/rfc/rfc2631.txt, last visited 1999.

[29] Rosenberg J, Schulzrinne H, Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., and Schooler E., "Session Initiation Protocol (SIP)," available at: http://www.hjp.at/doc/rfc/rfc3261.html, last visited 2002.

[30] Schulzrinne H. and Rosenberg J. "The IETF Internet Telephony Architecture and Protocols," *IEEE Network*, vol. 13, no. 3, pp. 18-23, 1999.

[31] Strangio M., "Efficient Diffie-Hellman Two-Party Key Agreement Protocols based on Elliptic Curves," *in Proceedings of ACM Symposium on Applied Computing*, pp. 324-331, 2005.

[32] Subramaniam U. and Kuppuswami S., "A Biometric based Secured Session Key Agreement using Modified Elliptic Curve Cryptography," *The International Arab Journal of Information Technology*, vol. 12, no. 2, pp. 155-162, 2014.

[33] Walsh T. and Kuhn D., "Challenges in Securing Voice over IP," *IEEE Security and Privacy*, vol. 3, no. 3, pp. 44-49, 2005.

[34] Wang C., Li W., and Lian W., "A Distributed Key Changing Mechanism For Secure Voice Over IP (VOIP) Services," *in Proceedings of IEEE International Conference on Multimedia and Expo*, Beijing, China, pp. 895-898, 2007.

[35] Wang S., Cao Z., Strangio M., and Wang L., "Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman key Agreement Protocol," *IEEE Communication Letters*, vol. 12, no. 2, pp. 149-151, 2008.

[36] Yang C., Wang R., and Liu W., "Secure Authentication Scheme for Session Initiation Protocol," *Computer and Security*, vol. 24, no. 5, pp. 381-386, 2005.

[37] Yooni E. and Yoo K., "A New Elliptic Curve Diffie-Hellman Two-Party Key Agreement Protocol," *in Proceedings of the* 7th *International Conference on Service System and Service Management*, Tokyo, pp. 1-4, 2010.

Subashri Thangavelu received her BE degree in Electronics and Communication Engineering from College of Engineering, Guindy, ME degree in Applied Electronics and PhD from Madras Institute of Technology, Chennai. She was a recipient of academic exchange fellowship of Association of Common wealth Universities. She has carried out funded projects on Tracking Algorithm for ship borne RADARS-funded by LRDE; GPS signal simulator-funded by Ministry of Information Technology; University Micro satellite-funded by ISRO; Semantic Intrusion Detection System-funded by Xambala Inc. Multi Sensor Data and Image Fusion, Power optimization in Wireless Sensor Network-funded by TCS. Currently, she is a Professor and Head of Department of Information Technology, Madras Institute of Technology, Chennai. Her areas of interests are networking, parallel processing and embedded systems.

Vaidehi Vijaykumar received her BE degree in Electronics and Communication Engineering from Thiayagarajar College of Engineering, Madurai, ME degree in Communication Systems from Thiayagarajar College of Engineering, Kamaraj University, Madurai. Her areas of interests are networking, cryptography and network security, communication systems. Currently, she is pursuing her PhD from Anna University.