Development of Key Exchange Protocol to Enhance Security of Voice over Internet Protocol on Mobile Phone

Yoanes Bandung and Andri Priyatna Putra

School of Electrical Engineering and Informatics, Institut Teknologi Bandung
Bandung, Indonesia
ybandung@gmail.com, andripriyatnaputra@gmail.com

Abstract: A system of securing voice communication on mobile phone based on peer-to-peer SIP protocol (P2PSIP) is discussed in this paper. This paper presents a new key exchange protocol for secure Voice over Internet Protocol (VoIP) communication on mobile phones with P2PSIP. In this paper, security threats and issues in VoIP are analyzed. In our approach, we combine key exchange protocol based on the Elliptic Curve Diffie Hellman (ECDH) public key cryptography with identity based user's authentication, beside we use existent text message to exchange user information (identity, IP Address, and Port). The key exchange protocol is proposed to assure confidentiality and integrity of voice communication on mobile phone. We conducted security analysis between the proposed protocol with the existing ECDH protocol and compared their performance of key generating and key exchange time. The proposed method was validated by Scyther tool for proofing the proposed key exchange protocol. The experiment results showed that the combination of ECDH and authentication mechanism has proved to be secure against attacks. With the addition of the authentication scheme, total execution time of generate key and exchange key is slower by 11.70% than those of the original ECDH. Although the execution time run more slowly, we can guarantee that the VoIP communications still can be performed interactively without impairments because the key exchange process is carried out before communication between two peers begins. We conducted the confidentiality and integrity examination using Wireshark and Mean Opinion Score (MOS). Results of the Wireshark tool show that the VoIP communication is secure againts attacks. From the MOS measurements we obtained score 3.6 which means we achieve good quality and integrity of VoIP communication.

Keywords: VoIP Security, P2PSIP, Key Exchange Protocol, ECDH, Scyther Tool

1. Introduction

Nowadays the information technology (IT) has been used as one of the most important things in human life. The rapid changes in today's information era have been faced by all organizations. It is shown that the entire organizations use the IT in all their activities, including the search of information and communication via internet technology. The internet is the largest system of connected computers around the world which people use to communicate with each other [1]. One of the methods used to communicate over internet technology is Voice over Internet Protocol (VoIP). VoIP is a method for transmitting voice as packets over the internet protocol [2]. Various reasons were put forward by organizations in the implementation of VoIP. One of the many reasons in the application of VoIP is cost savings including hardware requirements, training costs, the potential cost of electrical energy, and loss of business at a transitional stage [3]. Moreover, the adoption of VoIP can help reduce business costs through reducing operational cost, reducing maintenance costs, and reducing network infrastructure cost [4]. In other words, the key advantage of VoIP is low cost; it can integrate data, voice, and video in single network environment [5].

In the last decades, mobile devices have evolved from a device that only used to communicate into a multifunction device. The use of mobile devices has grown rapidly worldwide, especially Android-based smartphone. The growth of Android-based smartphone

Received: August 10th, 2016. Accepted: March 20th, 2017
DOI: 10.15676/ijeei.2017.9.1.12

users are very broad, Chief Executive of Google Inc. Sundar Pichai said that until September 2015, Android users has reached 1.4 billion, up 400 million users since May 2014 [6].

In the past few years, VoIP has developed rapidly and widely used. According to the works of [7], several VoIP protocols such as Session Initiation Protocol (SIP) [8], Inter-Asterisk eXchange (IAX) [9] and H.323 [10] still do not provide any form of security for the voice communication. Recently, some research works like in [11], [12], [13], and [14] have focused on peer-to-peer (P2P) in SIP instead the use of SIP servers to establish VoIP communications. A standard P2PSIP is currently being designed by the P2PSIP working group (WG) [11] in the Internet Engineering Task Force (IETF) to enable the discovery of resources that can be distributed in a SIP network and to eliminate or to reduce the need for a centralized server [12]. A typical P2P VoIP session contains two steps: P2PSIP signaling establishment and Real-Time Transport Protocol (RTP) media session transmission [13]. P2PSIP presents new security issues in terms of resource confidentiality, integrity, availability, consumption, latency, and peer lifetime [14].

However, in addition to the benefits provided by the VoIP that utilizes internet protocol network, VoIP also has disadvantage of the low level of security compared to the conventional communication system [15]. Team X-Force Internet Security Systems found a weakness in the security of VoIP that the application would give attacker the ability to listen or divert calls, in addition to gain unauthorized access to network which running VoIP [15]. One of the threats and vulnerabilities in VoIP is interception by unauthorized parties which person without any permission or approval can access the VoIP communication system.

The proposed security mechanism is an enhancement of the previous research [7]. Our proposed work is VoIP security mechanism based on the improved Elliptic Curve Diffie-Hellman (ECDH) and identity based authentication. In the previous works, ECDH is used to protect voice calls on mobile phone over VoIP server. ECDH mechanism is implemented in one of famous open source application for VoIP server, Asterisk PBX Server. The secret key was used between client softphone like Sipdroid/Linphone and Asteriks PBX Server. Therefore, they used common authentication method between client and server. In their case, they used ID and password that were stored in server. One of the common threats if we store username or ID and password in a server is the famous brute force attack, more over if we store the ID and password in plain text format.

In our method, we proposed new approach that there is no more storing username and password in the server. An identity based authentication will be applied as a replacement of the common certificate-based authentication scheme. We also conducted an experiment to prove the proposed protocol by using the Scyther tool [16] to analyze its security properties and its structure. Moreover, we also conducted an experiment to examine the confidentiality by using the Wireshark tool [17] and integrity of VoIP communication by using Mean Opinion Score (MOS) [18] approach.

2. Related Works

Developing a secure authentication protocol is one of serious issues in SIP-based communication services. To date several protocols have been suggested to seek ways of strengthening the security of SIP authentication process. Kilinc et al. [19] identified, categorized, and evaluated various SIP authentication and key agreement protocols according to their performance and security features. The proposed SIP authentication is categorized into four sections: Password Authenticated Key Exchange (PAKE) based, hash and symmetric encryption based, Public Key Cryptography (PKC) based, and identity based schemes. Performance of the hash and symmetric encryption is considerably better than other schemes, but it has some security weaknesses.

In the literature, several key exchange protocols have been proposed in order to strengthen the security of VoIP based on SIP [20], [21], [22], most of which are based on Elliptic Curve Cryptosystem (ECC). In general, ECC is public key cryptography that can be used for implementing digital signature or key agreement. The most benefit of ECC is smaller key sizes

and more efficient implementation at the same level security compared with other famous schemes such as RSA.
The standard Elliptic Curve is defined as the equation [7]:

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

where $a, b \in F_q$ and $4a^3 + 27b^2 \neq 0$.

In general, value of 'a' and 'b' provides a different construction of the Elliptic Curve. All points (x, y) that fulfill the above equations and the point at infinity thrust on the Elliptic Curve. On the curve, the public key is a point and the private key is a random number. The public key can be obtained by multiplying the private key with G the generator point in the curve [7]. The domain parameter of ECC consists of the generator point G and the curve parameters 'a' and 'b. Point Multiplication is one operation that is involved in ECC, which is the multiplication of Private Key (n_A, n_B) with Base Point (G) to obtain Public Key (P_A, P_B). Point Multiplication is obtained by two elliptic curve operations which is point addition and pointdoubling. The point multiplication makes the elliptic curve cryptography is more secure than the other crypto systems because of its new key point at every time. Research work on [23] has proposed privacy of voice calls for VoIP communication. It used the basic ECDH key exchange protocol. ECDH is variant of Diffie-Hellman scheme that uses elliptic curve cryptography. Since the previous work used basic authentication between client and SIP server, in this case is PBX server, the adversaries can easily carry out the attack, especially brute-force attack to exploit id client and password. The basic ECDH that has been used by previous research is shown in Figure 1.

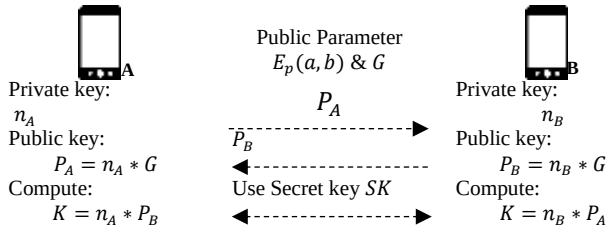


Figure 1. Basic ECDH Key Exchange Mechanism [13].

One of the advantages of ECDH is smaller key size. The computational complexity to break the ECDH protocol based Advanced Encryption Standard (AES) [24] key is much higher than DH based AES key. Computational complexity to break the key will rise rapidly in both algorithms when the key sizes increase. The parameters belong to the equation should confirm to the specific Elliptic Curve recommended by NIST [25] in order to resist attacks. Table 1 shows the NIST Guidelines for public key sizes for AES. To encrypt and decrypt data, current AES systems use a 1024 bit RSA cipher. A higher level of complexity is achieved using a 256 bit ECDH key which is smaller and more efficient than the RSA key. The smaller key sizes result in reduced time for encryption and decryption [7].

Table 1. NIST Guidelines for Public Key Sizes for AES [7].

ECC Key Size (bits)	RSA/DH ($\sqrt{n}$)	Key Ration Size
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15360	1:30

Since our VoIP communication is based on P2PSIP, it means our communication model does not use any server as a gateway or proxy. In our proposed work, we use the user's identification information $(ID, IPAddress, Port)$ for the authentication. Our works focus on

the usage of ECDH key exchange protocol with the combination of user identity authentication. Moreover, our works focus on the use the existing phone number and exchanging information via SMS or text message to attain the objectives generating key and more secure system.

3. Proposed Secure VoIP Communication Scheme

This section describes proposed secure VoIP communication scheme. The proposed scheme consists of three phases: information exchanging, authenticated key exchange, and voice data encryption. The notations used in this paper are defined in Table 2. The notations consist of public parameter such as identity (ID_A, ID_B) which means identity of user agent A and B, IP address (IP_A, IP_B), and Port ($Port_A, Port_B$). The other notations used for ECDH key exchange and authentication scheme.

Table 2. Notations

Notation	Description
ID	Identity of user agents (Phone Number e.g +62856XXXXXXX)
a, b	Pseudorandom number
p	Random prime number
IP_A, IP_B	IP Address user agent
$Port_A, Port_B$	Port user agent
P_{IA}, P_{IB}	Public information user agent
h	Hash function
Pub_A, Pub_B	Public parameter for user agent A,B
SK, SK_A, SK_B	Shared secret key of user agent A & B
$\oplus$	XOR operation
F_p	A prime finite field
$E_q(a, b)$	Elliptic curve over finite field
G	Base point

1. Information exchange

In this section, we present our approach based on existing infrastructure of mobile phone users' provider for exchanging public information. We use a Short Message Service (SMS) to exchange several parameters, such as user's identity, IP address and port. Figure 2 shows the process of exchanging information parameters using SMS. Firstly, Alice sends her identity (ID_A) and other parameters (IP address and Port) to Bob. Bob receives and saves Alice's parameter and send his parameters (IP address and Port) to Alice. Alice and Bob keep their parameter that will be used in authentication mechanism.

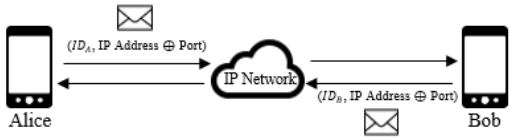


Figure 2. Proposed Information Exchange uses SMS.

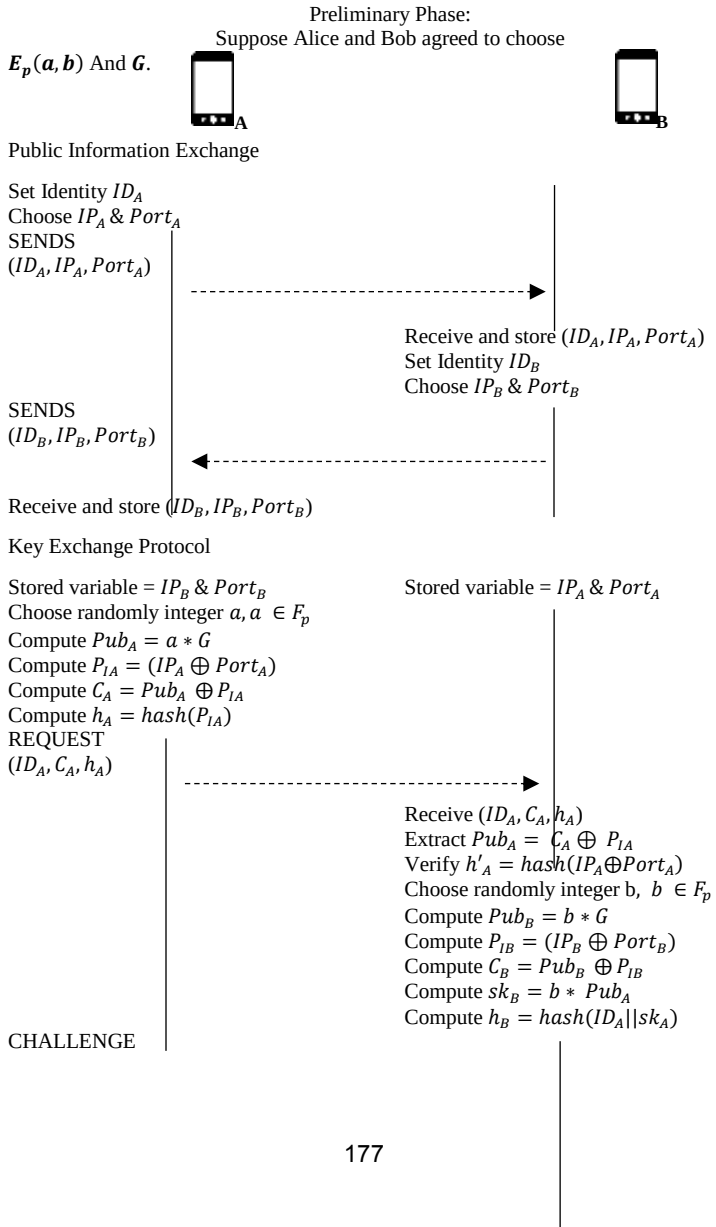
2. Key Exchange Protocol

This section describes the authentication key exchange protocol for P2PSIP based on ECDH with a user's identity based authentication consists of user's identity, IP address and port. The authentication is used to ensure the key exchange protocol runs between user agent to obtain voice conversation. This proposed scheme has the advantages of public key cryptography. Figure 3 shows the proposed key exchange protocol based on ECDH and user's identity authentication. We suppose that both Alice and Bob have access to ECDH parameters ($E_p(a, b)$, G) and intend to agree on shared secret key SK. In the initial session setup between client, Alice selects an integer randomly a with $a \in F_p$, computes $Pub_A = a * G$, computes

$P_{IA} = (IP_A \oplus Port_A)$ which means this is XOR operation between IP_A and $Port_A$, computes $C_A = Pub_A \oplus P_{IA}$, computes $h_A = hash(P_{IA})$ then sends a $REQUEST$ message include (ID_A, C_A, h_A). Bob receives the Alice's parameters, then derives Pub_A with extract $Pub_A = C_A \oplus P_{IA}$, verifies $h'_A = hash(IP_A \oplus Port_A)$, if true then Bob selects an integer b with $b \in F_p$, computes $Pub_B = b * G$, then computes $P_{IB} = (IP_B \oplus Port_B)$, computes $C_B = Pub_B \oplus P_{IB}$, computes $SK_B = {Pub_A}^b * b$, computes $h_B = hash(P_{IB})$ then sends an $CHALLENGE$ message include (ID_B, C_B, h_B). Alice receives Bob's challenge message then derives Pub_B with extract $Pub_B = C_B \oplus P_{IB}$, computes $SK_A = {Pub_B}^a * a$, computes and verifies $h'_A = hash(IP_A \oplus Port_A)$. If the verification of h'_A is true then Alice sends $RESPONSE$ message include (ID_A, h'_A). Bob verifies $h'_A = h_B$. If the verification of h'_A is true then both Alice and Bob share secret key SK to each other.

3. Voice Data Communication

In our proposed scheme, the voice packet is encrypted with AES encryption algorithm [27] using exchanged shared key SK and send it to another user for the secured VoIP network. The receiver decrypts the received voice packet using the same shared key SK. This key is used in order to protect users' privacy and data confidentiality.



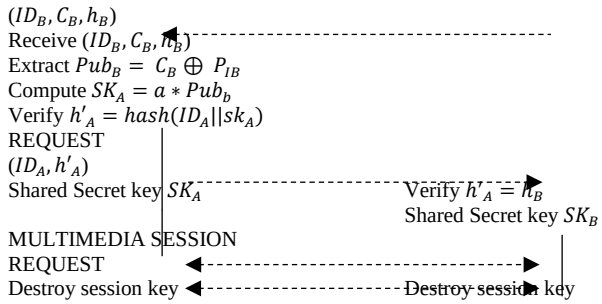


Figure 3. Proposed P2P Key Exchange Protocol

Figure 4 shows an overall flow chart of proposed voice communication protection scheme. The flow consists of three phases: information exchanging phase, key exchange phase, and secured media communication.

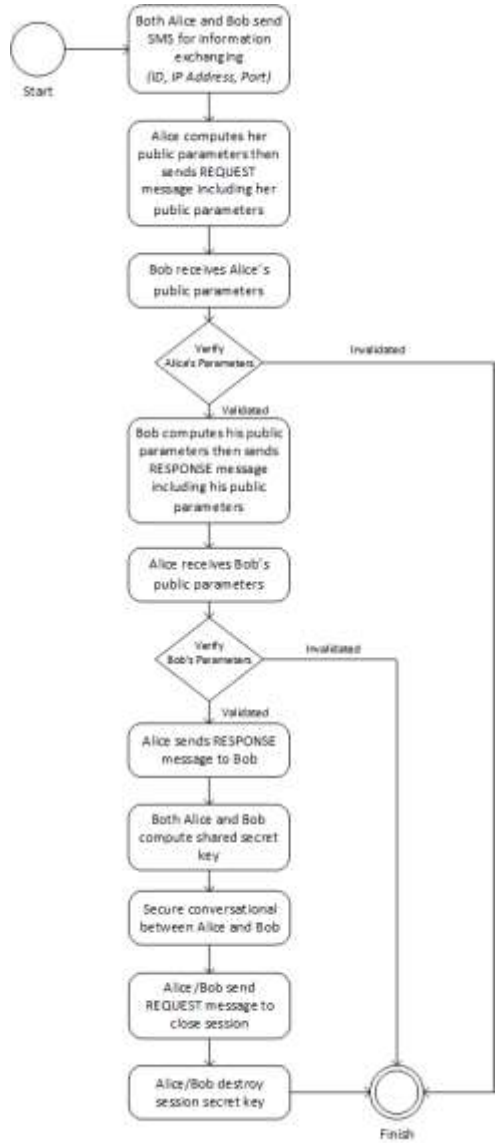


Figure 4. Overall Flow Chart Proposed Secure Voice Communication

4. Result

A. *Security Analysis of The Proposed Key Exchange Protocol*

In this section, we present security analysis of the proposed authenticated key exchange agreement protocol related to several security issues as follows.

a. Replay Attacks

The proposed scheme can resist the replay attack. Suppose an attacker Eve intercepts $REQUEST\ (ID_A, C_A, h_A)$ from Alice and replays it to impersonate Bob. However, Eve cannot compute the correct secret key SK and deliver it to Alice. When Eve tries to guess the secret key SK from the intercept request message C_A, Eve still faces the discrete logarithm problem [28].

b. Dictionary Attacks (offline password guessing attack)

In our scheme, the key exchange protocol does not require a password. An attacker Eve can intercept the $REQUEST\ (ID_A, C_A, h_A)$ but Eve still has to extract $C_A = Pub_A \oplus P_{IA}$ which is the same way to solving discrete logarithm problem (DLP). Therefore, Eve cannot launch the offline dictionary attack.

c. Man in the middle attack

The proposed scheme can resist against the man-in-the-middle attacks. An information exchange scheme and authentication $hash(IP_A \oplus Port_A)$ or $hash(IP_B \oplus Port_B)$ is used to prevent the man-in-the-middle attacks. The illegal attacker Eve cannot pretend to be each user agent authenticate the message.

d. Modification Attack

The proposed scheme can resist against the modification attacks. An attacker Eve may intercept the message that being transmitted over insecure network and tries modify $Pub_A, h(ID||SK_{AB})$, the Eve has to validating the $h(ID||SK_A)$ and $h(ID||SK_B)$.

e. Mutual Authentication

The proposed scheme can provide mutual authentication. In our scheme, each users authenticate each other by checking $h'_A = hash(IP_A \oplus Port_A)$ dan $h_B = hash(ID_B||SK_B)$. Therefore, our protocol can provide mutual authentication.

B. *Performance Evaluation*

This section describes performance evaluation of the proposed key exchange protocol that includes measuring of three performance parameters: processing time, confidentiality, and integrity.

B.1 Processing Time

In this sub-section, we evaluate the time needed to execute the key exchange compared with existing ECDH key exchange protocol. The need of time measurement is to check the efficiency of proposed scheme. The simulation was conducted on android based operating system, written in Java and maintained in Eclipse with the following configuration: processor dual core 1.4Ghz, 1 GB memory RAM, and Android 4.0 KitKat operating system for the first device, second device runs Intel® AtomTM x5-Z8550 1.4Gz, 2 GB memory RAM and Android 6.0 Marshmallow operating system. For each method, execution time was measured 50 times repeatedly. The average value of the measure values was calculated and used to compare. In our works, we calculate the time needed for generating key and time needed of computing the shared secret key for each user. The execution time consists of key generating time and secret key computing time. As seen in the Table 3, the proposed key exchange protocol shows decrement of the total execution time by 213.66 ms to 238.66 ms which means the execution time is larger by 11.70 % in the implementation of the scenario on Android based

devices. We observed that the addition of authentication scheme makes the execution time larger.

Table 3. Execution Time Result.

Method	Existing Scheme (ms)	Proposed Scheme (ms)
Generate Key	117.44	134.72
Compute shared secret key	96.22	103.94
Total	213.66	238.66

According to the measurement results, the proposed key exchange protocol was slower than the existing protocol due to the addition of authentication method with some additional cryptography function such as XOR and hash function.

B.2 Confidentiality

This section describes verification of our protocol using Scyther Tool [27] and Wireshark. Scyther is one of commonly tools for verifying and characterizing security protocols. The Scyther tool [16] uses Security Protocol Description Language (SPDL) [26] language for writing protocol. We implemented the proposed protocol and the previous protocol in Scyther tool to see the differentiation between them. Figure 5 and 6 shows the differentiation result between ECDH and our proposed key exchange protocol.

Figure 5. Result of Previous Key Exchange Protocol.

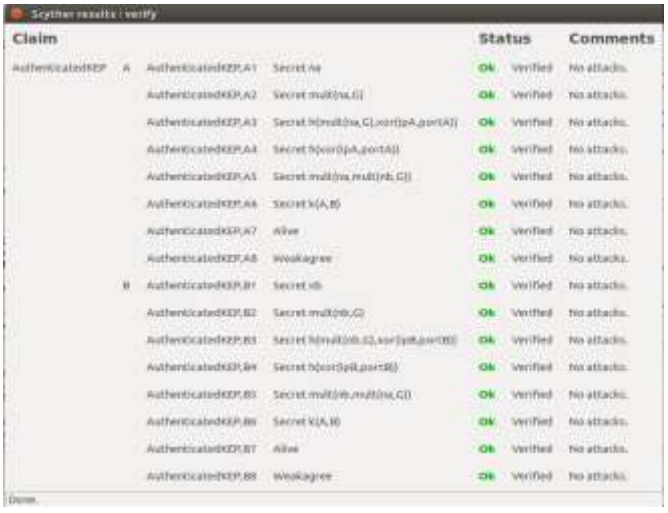


Figure 6. Result of Proposed Key Exchange Protocol.

We also compared the performance of communication between VoIP communication with encryption and without encryption. The aim of this examination to show the security of VoIP communication such as confidentiality and integrity. This confidentiality examination uses the sniffing method to capture the RTP packet of VoIP using Wireshark tool. Figure 7 shows the examination confidentiality scenario. There are two user agents, Alice and Bob that will be in the conversation. We put the Wireshark tool to capture their conversation in the middle of them.

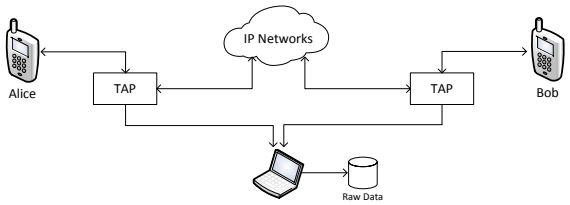


Figure 7. Scenario of encrypted VoIP examination.

Figure 8 and 9 shows the differentiation patterns between conversation without any encryption and conversation with encryption. Therefore, Wireshark tool results that the conversation is secure against eavesdropping.

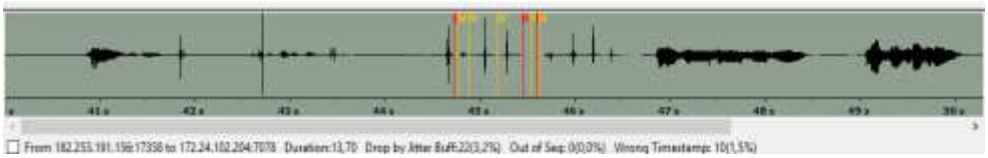


Figure 8. Wireshark Sniffing Result Conversation Without Encryption.

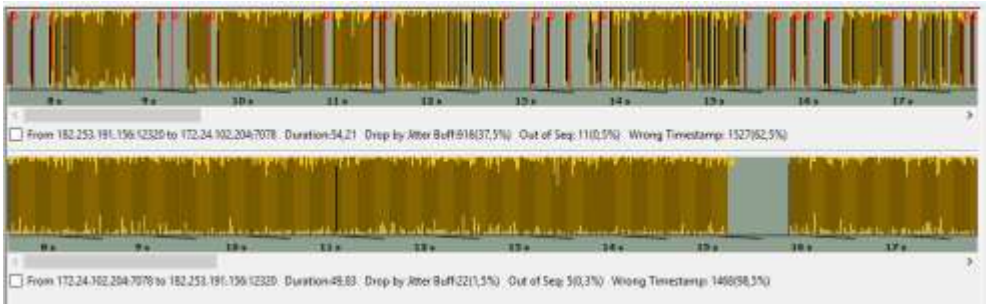


Figure 9. Wireshark Sniffing Result Conversation With Encryption.

Table 4 shows a comparison of several functionally security issues as described on the preceding section between the proposed protocol and the previous protocol [23]. It is shown that the proposed protocol could not only secure against several attacks, but it also provides mutual authentication feature and does not require password verification as the protocol uses P2PSIP that no centralized server is needed.

Table 4. The Functionally Comparison Between Proposed Protocol And Previous Protocol

Security Attack and Feature	Previous Work [23]	Proposed Work
Replay Attack	Yes	Yes
Offline guessing attack	N/A	N/A
Man in the middle attack	No	Yes
Modification Attack	Yes	Yes
Mutual authentication	N/A	Yes
Password verification	Yes	N/A

B.3 Integrity

For integrity checking, we used MOS to validate the conversation between sender and receiver. The user's perception is expressed in MOS values. ITU-T P.800 [18] has established the recommendation in telephony networks to obtain the human user's view of the quality of the network and the estimated MOS. We conducted the examination in this integrity test to around 10 listeners, the 6 (six) listeners gives value 4 for the conversation score, other listeners gives value 3. Thus, the average MOS result is 3.6 that the quality of VoIP delivery achieves good quality. As a consequence, we achieve the integrity of the VoIP conversations.

5. Conclusion

In this paper, we proposed an enhanced of the key exchange protocol in ECDH with the addition of authentication mechanism by adding identity (phone number), IP Address, and port for each user. We validated the proposed key exchange protocol by comparing its performance with previous key exchange protocol in ECDH. Validation was done by implementating of the proposed work on mobile devices based on Android operating system. We also use the Scyther tool to verify our proposed security protocol, Wireshark tool to perform sniffing method to capture voice packet, and MOS subjective test to obtain the integrity of voice conversations. Moreover, we compared the time needed for generating key and compute the shared secret key between proposed protocol and previous protocol. The results based on Scyther tool are combined with manual analysis, our proposed protocol has been verified and all the roles and characterization of the protocol was totally secure compared with the previous protocol that has disadvantage of man in the middle attack. The result of the overall execution time of proposed protocol is slower by 11.70% than that in previous protocol. The decrement of the performance is in consequence of addition of authentication mechanism with additional cryptography functions such as XOR and a hash function. Based on the results of Wireshark and MOS subjective testing, we can guarantee that the VoIP conversation still can be performed and secured although the time of key exchange performance has decreased.

For the future works there are still possibilities to optimize and enhance the proposed protocol to improve its performance. There are some interesting topics for future research, one of them is Quality of Service (QoS). In general, encryption in multimedia delivery especially VoIP is lowering quality. Therefore, study of QoS enhancement for secure multimedia delivery has to be done.

6. References

[1]. Cambridge University Press, “Cambridge Dictionary Online,” 2015.

[2]. R. Arora, “Voice over IP : Protocols and Standards”, [online], http://www.cs.wustl.edu/~jain/cis788-99/ftp/voip_protocols.pdf

[3]. Cisco, "*Cisco IP communications solutions*," vol. 2008, 2005.

[4]. NetLojix, "Voice Over IP Revolutionizing the way Businesses Communicate", vol. 2009, 2004.

[5]. E. T. M. Aire, B.T. Linde, L.P. , "Implementation Considerations in a SIP based secure Voice over IP Network", *Proceedings of 7th AFRICON Conference in Africa*, 2004, pp. 167-172.

[6]. The Wall Street Journal, “Google Says Android Has 1.4 Billion Active Users”. [online]. http://www.wsj.com/articles/google-says-android-has-1-4-billion-active-users-1443546856. Accessed December 2015.

[7]. Ashok. S, Arjun. A and T. Subashri, "Dynamic ECDH mechanism for enhancing privacy of voice calls on mobile phones over VoIP server", *Proceedings of International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, Ramanathapuram, 2014, pp. 1179-1184.

[8]. J. Rosenberg et al., “SIP: Session Initiation Protocol”, *RFC 3261, Internet Engineering Task Force*, June 2002.

[9]. M. Spencer et al., "IAX: Inter-Asterisk eXchange Version 2", RFC 5456, Internet Engineering Task Force, February 2010.
[10]. ITU-T Recommendation H.323, "Packet-Based Multimedia Communications Systems", *International Telecommunication Union*, December 2009.
[11]. P2PSIP Working Group. [online]. http://www.ietf.org/html.charters/p2psip-charter.html
[12]. Xianghan Zheng and Oleshchuk Vladimir. 2010. "A survey on peer-to-peer SIP based communication systems." *Peer-to-Peer Networking and Applications* 3 (4): 257–264.
[13]. Hua Jiang; Yongxing Jia; Xianru Du; Weizhi Wang, "An identity-based security mechanism for P2P VoIP," *Proceedings of 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS)*, pp.481-485, June 2010.
[14]. S. Touceda, J. M. Sierra, A. Izquierdo and H. Schulzrinne, "Survey of Attacks and Defenses on P2PSIP Communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 3, pp. 750-783, Third Quarter 2012.
[15]. F. G. Taylor. VoIP Security – Attacks and Solutions. Information Security Journal: A Global Perspective, 17(3), pp. 114-123.
[16]. Scyther Tool. [online]. http://www.cs.ox.ac.uk/people/cas.cremers/scyther/index.html
[17]. "Wireshark homepage, " http://www.wireshark.org/, Last accessed on 20 July 2016.
[18]. International Telecommunication Union. (1996) ITU-T Rec. P.800. [online]. http://www.itu.int/rec/T-REC-P.800/en
[19]. H. H. Kilinc and T. Yanik, "A Survey of SIP Authentication and Key Agreement Schemes," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1005-1023, Second Quarter 2014.
[20]. L. Ni, G. Chen and J. Li, "A Pairing-Free Identity-Based Authenticated Key Agreement Mechanism for SIP," *Network Computing and Information Security (NCIS), 2011 International Conference on*, Guilin, 2011, pp. 209-217.
[21]. S. Zhu, F. Yang, L. Zhang, S. Tang and J. Li, "ECC-Based Authenticated Key Agreement Protocol with Privacy Protection for VoIP Communications," *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, Beijing, 2013, pp. 2114-2118.
[22]. J. Zheng and D. Wang, "Cryptanalysis and improvement of a SIP authentication scheme," *Information Technology and Electronic Commerce (ICITEC), 2014 2nd International Conference on*, Dalian, 2014, pp. 199-203.
[23]. D. Perez-Botero and Y. Donoso, "VoIP Eavesdropping: A Comprehensive Evaluation of Cryptographic Countermeasures," *2011 Second International Conference on Networking and Distributed Computing*, Beijing, 2011, pp. 192-196.
[24]. National Institute of Standard and Technology, Advanced Encryption Standard, NIST FIPS PUB 197, 2001.
[25]. NIST. "Recommended Elliptic Curves for Federal Government Use", July 1999.
[26]. Dalal, N., Shah, J., Hisaria, K. and Jinwala, D. (2010) *A Comparative Analysis of Tools for Verification of Security Protocols.*
[27]. Basin, D., Cremers, C. and Meadows, C. (2009) LTL Model Checking Security Protocols. Journal of Applied Non-Classical Logics, 194, 403-429.
[28]. S. M. Kevin, "The Discrete Logarithm Problem", *Cryptology and Computational Number Theory* 42 (1990): 49.

Yoanes Bandung received the B.E., M.E., and D.E. degrees in Electrical Engineering from Institut Teknologi Bandung (ITB), Indonesia, in 2000, 2002, and 2008, respectively. In 2009, he joint the School of Electrical Engineering and Informatics ITB as a lecturer and affiliated with Information Technology Research Group. In 2014, he was a post-doctorate researcher in Department of Computer Science and Engineering, Frederick University of Cyprus through the Erasmus Mundus STRoNG-TiES Program. He is a member of the Institute of Electrical and Electronics Engineers (IEEE). His research interests are in the areas of multimedia communication, quality of service (QoS), and information security engineering.

Andri Priyatna Putra graduated from Universitas Komputer Indonesia (UNIKOM), Bandung and received Bachelor Degree in Informatics Engineering in 2008. In 2016, He received Master Degree in Informatics from Institut Teknologi Bandung (ITB). Currently, He works at private multinational corporation in Bandung which has been seconded as a part-time lecturer at Universitas Komputer Indonesia (UNIKOM). His research interests are computer networking and information security.