Performance Analysis of VoIP Client with Integrated Encryption Module

Abdi Wahab[1], Rizal Broer Bahaweres[1,3], Mudrik Alaydrus[1], Muhaemin[2], Riyanarto Sarno[4]
[1]Graduate Program of Electrical Engineering Department, Mercu Buana University, Jakarta, Indonesia
[2]Dept. of Information Systems, STMIK Indonesia, Jakarta, Indonesia
[3]Dept. of Informatics Eng., Faculty of Science & Tech., UIN, Jakarta, Indonesia
[4]Dept. of Informatics Eng., Faculty of Information Tech., ITS, Surabaya, Indonesia
Email:
nangdul56@gmail.com[1], rizalbroer@ieee.org[1,3], mudrikalaydrus@yahoo.com[1], muhaemin98@gmail.com[2], riyanarto@if.its.ac.id[4]

Abstract— **The number of VoIP users in Indonesia is very low, although the cost offered by VoIP is smaller than using pulsed phone. One of the reason is security provided by the VoIP service provider is still lacking. VoIP users have not received yet the security service to ensure the security of communications. This study tries to secure communications between VoIP users using encryption module that is integrated with VoIP client Sipdroid running on Android Smartphone. It is possible for VoIP users because VoIP client that can only be accessed by VoIP users. The result obtained after integration with encryption module using three encryotion schemes, they are AES, DES, and RC4. Sipdroid able to resist passive attack from tapping information (eavesdropping) during the communication session. And the result of QoS measurements is an increase delay of 0.01 ms and no significant change in the throughput and the packet loss, for throughput generated about 78 kbps, and for the average packet loss is 0.8%. However there is a noise that follows the communication on Sipdroid integrated with the encryption module due to the wave skew from the increase time during the encryption process.**

Keywords—VoIP; VoIP Client; Encryption

I. Introduction

Internet users are increasing in Indonesia based on the results of a survey of Communication and Information Technology in 2011 has increased very rapidly once. The largest percentage of 97.69% used the Internet to send and receive email, while the lowest is the promotion of the hotel followed by VoIP with each percentage of 0.14% and 13.54% [1].

If seen from the survey results, VoIP usage in Indonesia is still low, although many references are made to the advantages of VoIP in terms of lower costs compared to a conventional telephone. Besides having advantages, there are also disadvantages of VoIP. The weakness that still often happens is the sound quality is not good when compared to a conventional telephone. In addition to both of them, the problem of security is also a lot of reasons why VoIP users haven't used yet it. This is because the user does not get a good guarantee from the VoIP service provider, unless the company genuinely committed to providing VoIP services may have guarantee for the communication held by VoIP users. The possibility of attacks against VoIP servers by tapping (eavesdropping) can be happen anytime.

VoIP users will not be able to get access to the VoIP server provided by VoIP service provider, VoIP users can only use the VoIP client as a medium of communication and registration to the VoIP server. Perhaps a method to solve security issues is to secure the data communication to be sent from the VoIP client.

The purpose of this research is to integrate security features or modules or data encryption using multiple encryption methods such as AES, DES or RC4 on Sipdroid VoIP client when communicate through VoIP. And also to measure the performance of the VoIP client that has integrated security or encryption modules.

Getting VoIP client that has been integrated with the encryption module with a good performance is the goal of this research. With an integrated encryption module is expected to secure the VoIP user communication.

The formulation of problem can be determined in this study are as follows:

- How to integrate a VoIP client running on smarthphone or mobile-based encryption module?
- How to measure the performance of mobile-based VoIP client that has been integrated with the encryption module?

Extents of the problem in this study are as follows:

- VoIP client application used is Sipdroid.
- The encryption method is trying to integrate are AES, DES, and RC4.
- Test bed will be held on the Android 2.3 (GingerBread).
- Network architecture using a WLAN, so the scope of communication is only done in the indoor.

978-1-4673-2821-0/13/$31.00 ©2013 IEEE

- This study was simply to integrate encryption module, but have not been able to check up to the encryption scheme used when communicate.
- The attack simulations carried out just as a passive attack or an attack just to listen to the information during communication (eavesdropping).
- This study has not been to examine the changes communication data that occur due to the encryption process.

II. Literature Review

A. Related research

Authors get some old research associated with this study. In the study conducted by Talevski et al [2], in his article entitled "Secure Mobile VoIP", and also research by Nakarmi et al [3]. The difference between author's research and the other researches depicted in Figure 1 below.

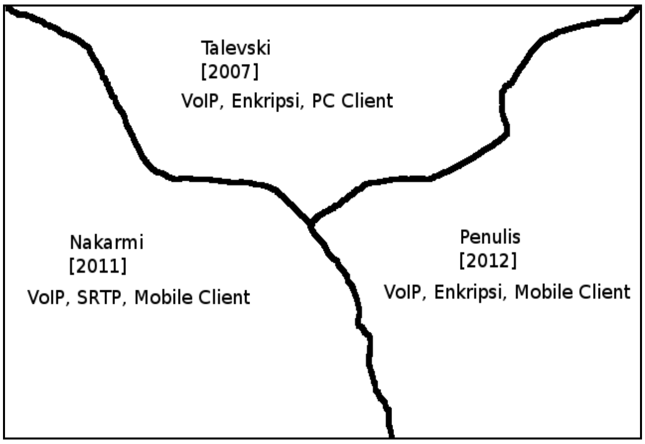
Talevski
[2007]
VoIP, Enkripsi, PC Client
Nakarmi
[2011]
VoIP, SRTP, Mobile Client
Penulis
[2012]
VoIP, Enkripsi, Mobile Client

Figure 1. The research description related to this research study.

Talevski trying to add encryption to the VoIP client module Kiax. Kiax is one of VoIP client that uses the protocol IAX (Inter-Asterisk Exchange), which resembles SIP and H323 protocols. Talevski integrate Kiax with encryption modules produced using Cryptlib library. Cryptlib contains cryptographic functions that can be integrated with the application. Encryption scheme used by Talevski is IDEA, RC4, and AES. Then, the results of Kiax which is integrated with encryption module was tested on a VoIP network using a LAN. The parameters taken are delay, jitter, bandwidth, and CPU performance. From the results obtained in the Talevski research, Kiax with AES CFB scheme is a scheme that selected compared to other schemes tested.

Other studies related to this research is the research of Nakarmi et al [2011], entitled "Evaluation of VoIP Media Security for Smartphones in the Context of IMS". In that research, Nakarmi explore alternatives and feasibility for VoIP media security for smartphones in the scope of the IP Multimedia Subsystem (IMS). And also, Nakarmi change Sipdroid to use SRTP and MICKEY-TICKET. SRTP is the Secure Real Time Protocol, and MICKEY-TICKET is a protocol for key exchange.

B. Sipdroid

Sipdroid is a voip client that runs on the Android operating system. Sipdroid uses the GNU Public License (GPL) v3, and can be downloaded for free from the Google Play or also from the website Sipdroid http://sipdroid.org. On the website can also be downloaded for Sipdroid source for users who want to modify or recompile Sipdroid.

Sipdroid using SIP (Session Initiation Protocol) protocol as a regulator of multimedia session initiation. And for the implementation Sipdroid using MjSip library.

C. Java Cryptography Extension (JCE)

JCE provides a framework and implementations for the algorithms of encryption, key generation and key agreement, and a message authentication code.

Supports symmetric encryption, asymmetric, block and stream ciphers. Also supports secure streams and sealed objects.

JCE API include:

- large symmetric encryption, such as DES, RC2, and IDEA.
- Symmetric stream encryption, such as RC4.
- Asymmetric encryption, such as RSA.
- Password-based encryption (Password-based Encryption).
- Key Agreement.
- Message Authentication Code (MAC).

Some basic cryptographic concepts that we use in this study, the authors take from the Stalling [4] and Schildt [5] books.

III. Research Methodology

The research methodology will be proposed in this research is as follows:

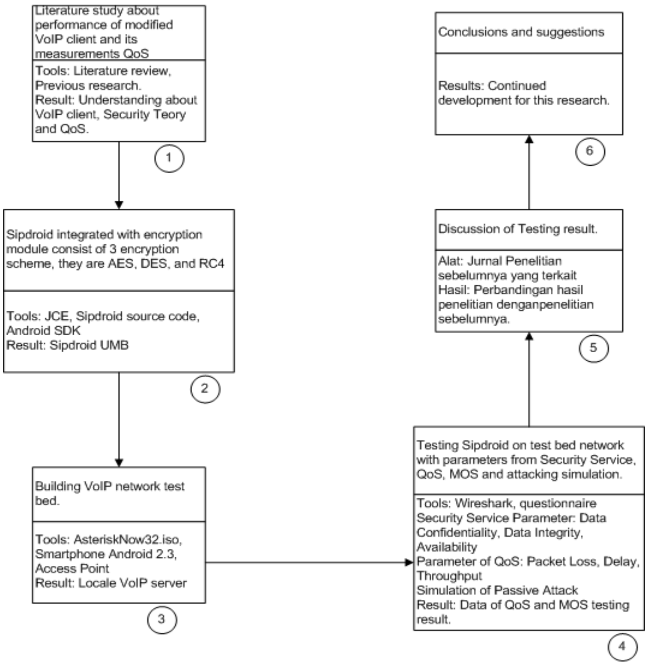
Literature study about performance of modified VoIP client and its measurements QoS
Tools: Literature review, Previous research.
Result: Understanding about VoIP client, Security Teory and QoS.
1
Sipdroid integrated with encryption module consist of 3 encryption scheme, they are AES, DES, and RC4
Tools: JCE, Sipdroid source code, Android SDK
Result: Sipdroid UMB
2
Building VoIP network test bed.
Tools: AsteriskNow32.iso, Smartphone Android 2.3, Access Point
Result: Locale VoIP server
3
Testing Sipdroid on test bed network with parameters from Security Service, QoS, MOS and attacking simulation.
Tools: Wireshark, questionnaire
Security Service Parameter: Data Confidentiality, Data Integrity, Availability
Parameter of QoS: Packet Loss, Delay, Throughput
Simulation of Passive Attack
Result: Data of QoS and MOS testing result.
4
Discussion of Testing result.
Alat: Jurnal Penelitian sebelumnya yang terkait
Hasil: Perbandingan hasil penelitian denganpenelitian sebelumnya.
5
Conclusions and suggestions
Results: Continued development for this research.
6

Figure 2. Research methodology

The methodology beginning with the research literature related to this research, then integrate Sipdroid with encryption module, building the test bed for VoIP networks, testing the result of integration Sipdroid with encryption module, the discussion of the test results, and finally conclusions and suggestions.

TABLE I. THE CORRELATION BETWEEN THE METHODS, DEVICES, PARAMETERS AND RESULTS

No	Methods / Techniques	devices	Parameter	result
1.	Making encryption scheme AES, DES, RC4	JCE	Lock, Data	Encryption Module with AES, DES, RC4.
2.	Sipdroid Integration with Encryption Module	Encryption Module, Source Sipdroid		Sipdroid integrated with encryption features.
3.	Making Network Test Bed	Smartphone Android, VoIP Server with Asterisk		Test bed VoIP network
4.	Testing Sipdroid with encryption features using Security Service.	Test bed VoIP network, Android Smartphone, Wireshark	Data confidentiality, data integrity, availability	Testing Data Security Service.
5.	Performance measurement Sipdroid with encryption features.	Wireshark, Test bed VoIP network, Android Smartphone, the survey.	Delay, packet loss, throughput, MOS.	Performance measurement data Sipdroid

A. Integrate Sipdroid with Encryption Module

For the next step, we will integrate the Sipdroid with encryption modules produced by JCE. Here is an illustration of the process of integration for encryption module into Sipdroid.

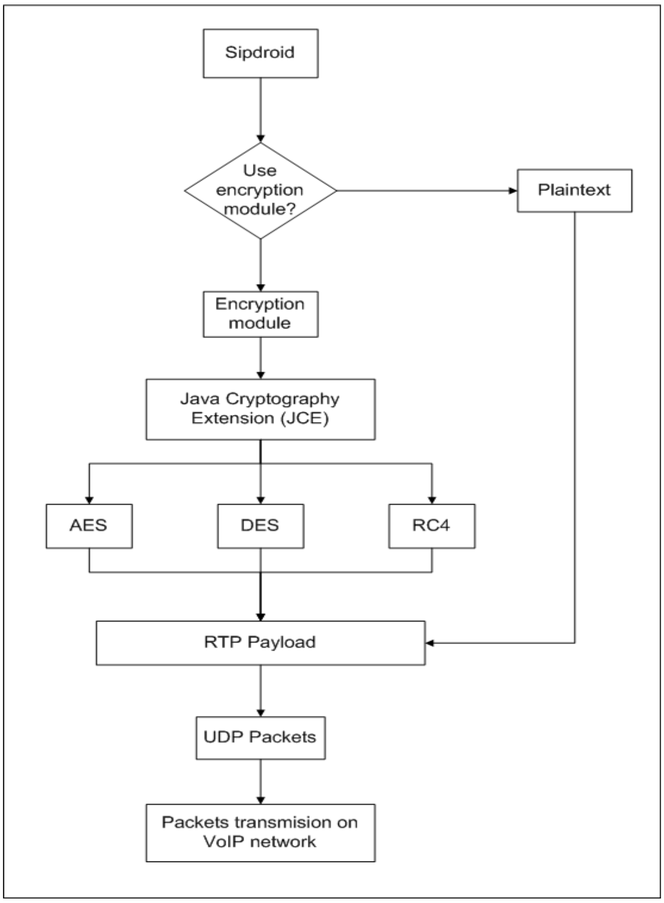

Figure 3. JCE integration process with Sipdroid

Stages of the process in Figure 3, the user can choose whether using or not using encryption module. If using encryption module, the user selects one of the encryption methods, namely AES, DES, and RC4. The encryption process is performed on RTP payload before it is wrapped into UDP packets and sent over the VoIP network.

So the activity of Sipdroid changed as shown below.

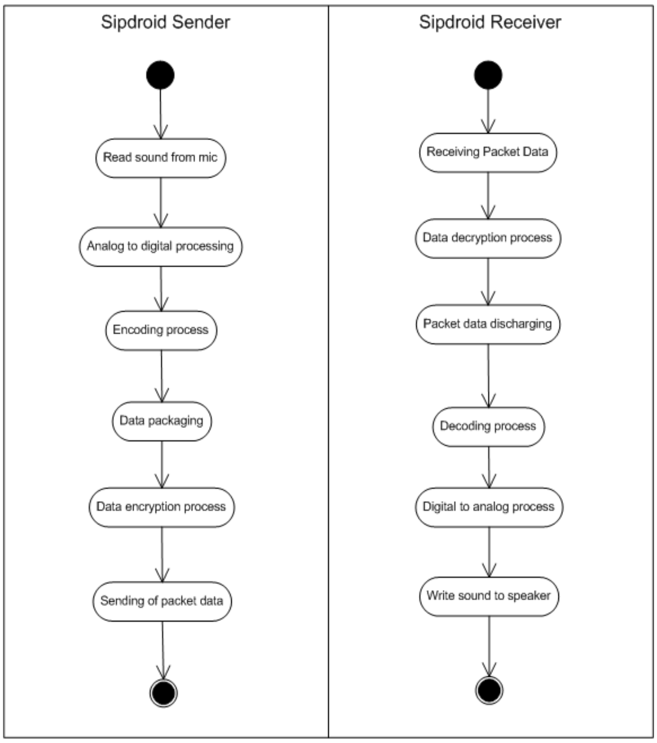

Figure 4. Modified Sipdroid activity diagram

On Sipdroid sender, there is a data encryption process on RTP packets to be transmitted, while the decryption process occurs on Sipdroid receiver. The received RTP packets will be decrypt.

B. *Design of VoIP Test Bed*

The Test bed for this research developed from Purbo book [6] will be illustrated in the following figure.

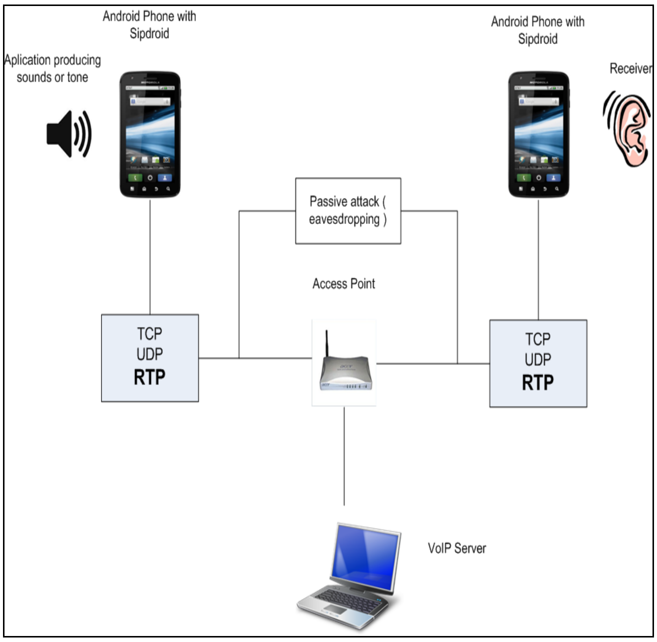

Figure 5. Test bed VoIP network

Test bed will be used only consisted of two smatrphone Android, communicated through a self-built VoIP server. Network using WLAN. For the measurement, to get the same sound, then we use the application generating the tone to do the automation of producing tone.

C. *Testing Scenario*

The first test scenario will use the parameters of delay, packet loss, and throughput, which took by the author from the book of Stalling [7]. Measurements done from end-to-end or on any Android smartphone using tools Shark [8]. Data is collected twenty times for each encryption scheme with the same key, and each communication session conducted over 15 seconds. Communication occurs only in one direction, and the resulting sound using application assistance, as shown in Figure 5. After QoS measurements, the next testing is Security service. The parameters for testing with security service are data confidentiality, data integrity, and availability.

IV. RESULT AND DISCUSSION

These are the results obtained in this research, using the parameters mentioned in section 3.3.

A. *Packet Loss*

Here is the result of average packet loss obtained from Sipdroid integrated with the encryption module.

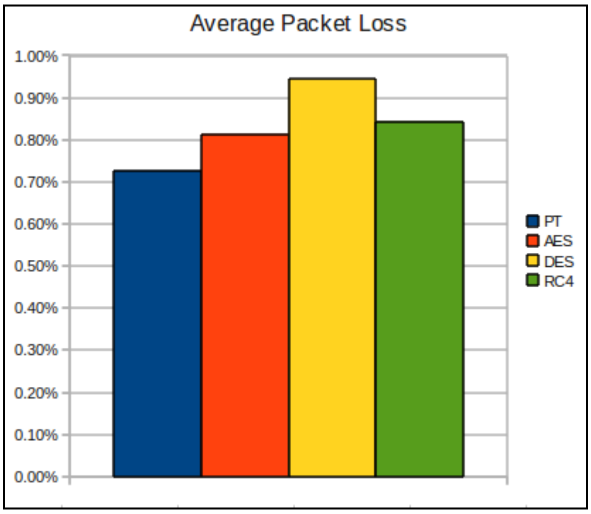

Figure 6. Average Packet Loss

The results of Figure 6 above illustrates that the normal Sipdroid has a least average packet loss compared with Sipdroid integrated with the encryption module. While Sipdroid with DES scheme has the biggest packet loss compared to the others. So that the best performance is still held by normal Sipdroid, followed by Sipdroid with AES scheme, in third position Sipdroid with RC4 scheme, and the last show poor performance is DES. Basically, VoIP communication especially with wireless networks will result packet loss.

The performance of packet loss shown in this result associated with communication often disconnected or not in a session. The results obtained above show that Sipdroid with AES become the best scheme among Sipdroid integrated with the encryption module.

B. Delay

The average result obtained during the measurement delay (delay of packet creation) is as follows.

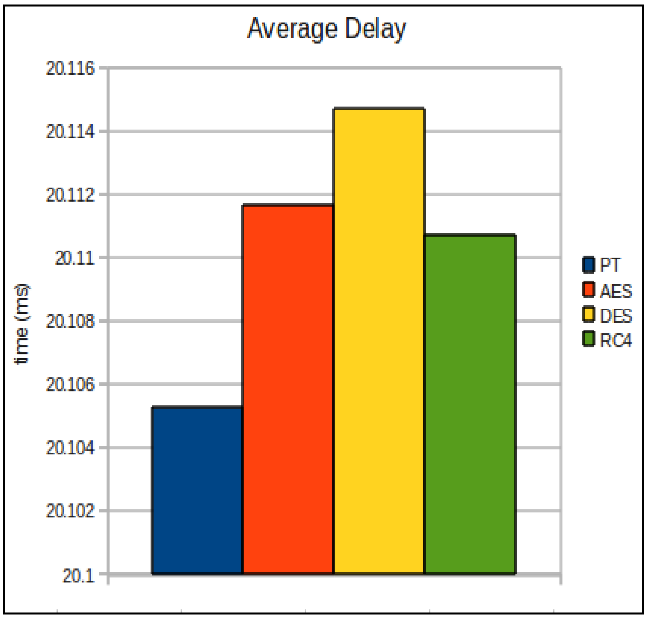

Figure 7. Average Delay

Figure 7 above shows the average delay of four schemes. Sipdroid normal had an average delay of the smallest compared to Sipdroid with encryption module. Differences delay which occurred about 0:01 ms for additions to the Sipdroid with encryption module. While in the Sipdroid with encryption module, Sipdroid with AES and RC4 scheme have a delay that is not much different, and for Sipdroid with DES scheme has the greatest delay.

From the result shown above, the delay differences occurs between normal Sipdroid and Sipdroid with encryption module due to encryption process on each packets to be transmitted from Sipdroid with encryption module. So, the delay measured in this research is a processing delay, not a transmission delay.

C. Throughput

Average throughput generated in this result are as follows.

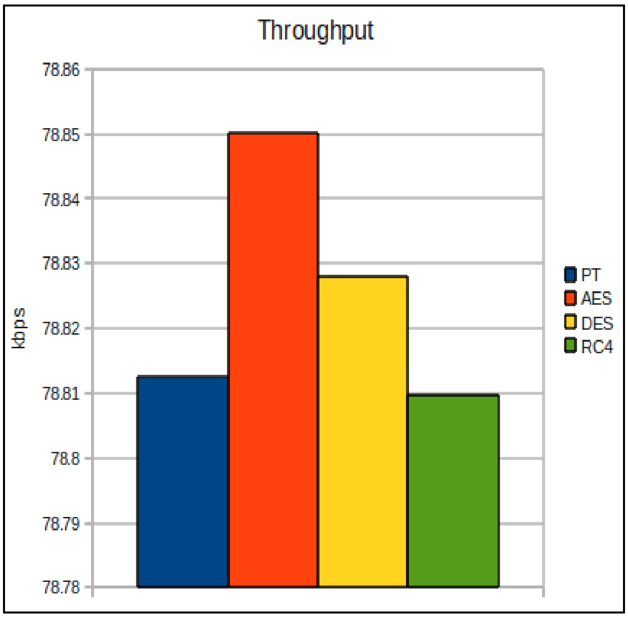

Figure 8. Average Throughput

Figure 8 above, shows the use of throughput used in the tested Sipdroid scheme. The range average of throughput about 78 kbps. The largest throughput produced by Sipdroid with AES scheme, while normal Sipdroid has a throughput that is not much different than the Sipdroid with RC4 scheme. And then Sipdroid with DES scheme lower than Sipdroid with AES scheme, or on the second place. The difference in throughput is due to the process of encryption or encryption algorithms used in process, in this process generate a package with a bit larger than the usual bit, especially on the results of the package generated from Sipdroid with AES and DES that change each packet length to 128 and 64 bit.

The results obtained on measuring throughput form this research, among Sipdroid integrated with the encryption module, Sipdroid with AES scheme is the best performance, with assumptions, greater throughput, the communication between VoIP users will be better. But this does not happen in normal Sipdroid, on normal Sipdroid, there is a good communication between VoIP users to communicate even when the resulting throughput smaller than Sipdroid with AES scheme.

D. Security Service

The testing with security services, they are data confidentiality, data integrity, and availability, having a good result. All of criteria of parameters can be fulfilled by Sipdroid integrated with encryption module.

E. Discussion

The results obtained from this research, especially from the three measurement parameters of quality of service (QoS) [9], namely delay, packet loss, and throughput, encryption schemes that proposed by researcher is AES scheme, although there is still noise generated from the encryption process.

And from Security Service parameters, the testing shown that Sipdroid integrated with encryption module is secure.

At the beginning of this study, researchers will try to simulate an attack to be carried out on Sipdroid integrated with the encryption module as in Figure 5. However, because of time, tools and space, the authors will continue to simulate the attacks in subsequent research.

V. CONCLUSION AND RECOMMENDATIONS

Conclusions of this research are as follows

- The encryption module generated from JCE encryption can be integrated well with Sipdroid by encrypting the RTP payload to be transmitted on a VoIP network.
- Measurement performance of security service for Sipdroid integrated with encryption module can be done well. It indicates that the integrated encryption module work well.
- QoS result from this measurement produce enlarged delay more than 0.01 ms for Sipdroid integrated with encryption module, mean while for packet loss and throughput there are no significance changes.
- Sipdroid with encryption module can overcome passive attack, because captured communication data by Wireshark can not be decoded well, this happen due to the encryption process in data.

And for recommendations for this research are as follows:

- Fixing the sound quality from Sipdroid integrated with encryption module.
- Adding a module to know encryption scheme in the beginning of VoIP communications.
- Analyze the payload data from encrypted RTP.
- Simulate an attack on Sipdroid integrated with encryption module.

REFERENCES

[1] ------------------. Hasil Survei Penggunaan Teknologi Informasi dan Komunikasi (TIK) di Sektor Bisnis Indonesia 2011. [On-line] Accessed in http://publikasi.kominfo.go.id/bitstream/handle/54323613/66/Hasil%20Survei%20TIK%20Sektor%20Bisnis%202011.pdf?sequence=1 on 15 Februari 2012.

[2] Talevski, A., Chang, E., & Dillon, T. (2007). Secure Mobile VoIP. Paper pada International Converence on Convergence Information Technology, Gyeongju, Korea.

[3] Nakarmi, P.K., Mattsson, J., & Maguire, G.Q. (2011). Evaluation of VoIP Media Security for Smartphones in the Context of IMS. Paper pada Swedish Communication Technologies Workshop, Stockholm, Swedia.

[4] Stallling, W. (2005). Crypthography and Network Security Priciples and Practices, Fourth Edition. Upper Sadle River: Prentice Hall.

[5] Schildt, H. (2002). Java 2: The Complete Reference, Fifth Edition. New York: McGraw Hill.

[6] Purbo, O. W., & Raharja, A. (2010). VoIP Cookbook. [On-line] Accessed in http://opensource.telkomspeedy.com/wiki/index.php/VoIP_Cookbook:_Building_your_own_Telecommunication_Infrastructure on 20 Januari 2012.

[7] Stalling, W. (2004). Computer Networking with Internet Protocols and Technology. Upper Sadle River: Prentice Hall.

[8] https://play.google.com/store/search?q=lv.n3o.shark&c=apps

[9] Amin, A. H. M. (2005). VoIP Performance Measurement Using QoS Parameter. International Converence on IIT, Dubai, UEA.