ANALYSIS OF EFFECT OF ZFONE SECURITY ON VIDEO CALL SERVICE IN WIRELESS LOCAL AREA NETWORK

Arip Solehudin [1]
Teknik Informatika Fakultas Ilmu Komputer
Universitas Singaperbangsa Karawang
Karawang, Indonesia
arip.solehudin@staff.unsika.ac.id

Bayu Priyatna [2]
School of Engineering and Computer Science
Universitas Buana Perjuangan Karawang
Karawang, Indonesia
bayu.priyatna@ubpkarawang.ac.id

Nono Heryana [3]
Sistem Informasi Fakultas Ilmu Komputer
Universitas Singaperbangsa Karawang
Karawang, Indonesia
nono@unsika.ac.id

***Abstract*—Along with the development of WLAN (Wireless Local Area Network) network technology, many services that used cable networks began to migrate to wireless networks. VoIP (Voice over Internet Protocol) is one service implemented in wireless local area networks. However, VoIP that uses wireless technology as a data stream media Video Call service has a high risk of tapping pictures. To avoid tapping pictures, you can add a security system to the service, one of which is to use Zfone security. With him adding a security system that will influence the work of Video Call services on the quality of service. The author uses the General Network Design Process (GNDP) study method. After testing security by intercepting images, Zfone affects the security of video calls on WLAN by changing conversations between client images to black. Although Zfone secured from eavesdropping on video calls, Zfone also impacted the deterioration of the quality of Video Call services. The results of quality of service before using the Zfone security system with the parameters of delay, jitter, and packet loss are as follows; the delay time value is 68.93ms, the jitter time value is 2.04ms and the packet loss parameter before using Zfone security is 0%. The results of quality of service after using the Zfone security system with the parameters of delay, jitter, and packet loss are as follows; the value of delay time is 80.12ms and the value of jitter time is 4.36ms on packet loss parameters after using Zfone security which is 0%.**

Keywords*—*VoIP, Zfone, Network Security, Quality Of Service, GNDP.

I. Introduction

The development of computer networks at this time which is rapidly making a big influence on the network technology itself, the current network technology that allows one to communicate with each other long-distance is like a necessity that can not be separated. One of the technologies used today is VoIP. Voice over Internet Protocol (VoIP) is a technology that allows long-distance voice conversations through internet media. In addition to conducting long-distance conversations over the internet, VoIP has a service that can carry out chat messages and even make video calls.

VoIP can also be implemented on a Local Area Network (LAN) or abbreviated as VoIP LAN. VoIP LAN networks are usually implemented on cable networks and combined with Public Switch Telephone Network (PSTN) networks. The development of network technology, the existence of VoIP LAN that uses cable began to move using wireless network technology, namely wireless. The use of wireless networks as a medium for the flow of data makes VoIP services can be used in several communication technology tools such as personal computers, laptops, and smartphones.

The use of VoIP technology that is implemented on WLAN networks with video call services found in VoIP facilities is an excellent solution for conducting conversations at affordable costs compared to the VoIP services associated with PSTN. The use of VoIP technology with video call services is very beneficial for the user, but communication that is so efficient and affordable costs in terms of security is less paid attention. Therefore, when making a video call service that is connected to a WLAN, it is still very vulnerable in terms of security because the network works by spreading radio frequency signals, allowing unauthorized parties to enter the network and intercept the ongoing communication. This needs to be addressed because it is a very important matter concerning user privacy.

Based on this, what can be done is to add a security system to the WLAN network. By using Zfone software that uses the Zimmermann Real-Time Transport Protocol (ZRTP) protocol as its executor. The use of Zfone is an alternative method for security by encrypting the data traffic of a WLAN. By implementing an additional security system using Zfone software, the data packet must go through several security stages before being sent and arrive at its destination.

II. Research Method

In this study the author uses the General Network Design Process (GNDP) method with 6 stages as follows:

1. *Assess needs and costs*

The initial stages of the General Network Design Process (GNDP) there are two main things as follows:

a. *Assessing Needs*

This stage explains what is needed by the user by doing this research. The elements of availability that must be achieved in this research are video call service security and Quality of Service WLAN network system.

b. This stage is the stage for the budget required in this research both from hardware (hardware) and software (software)

2. *Choosing topology and technology*

This stage is the stage for the selection of topology and technology used in this research. In this study using the star topology. The wireless network in this study uses infrastructure mode, presented in Figure 1.

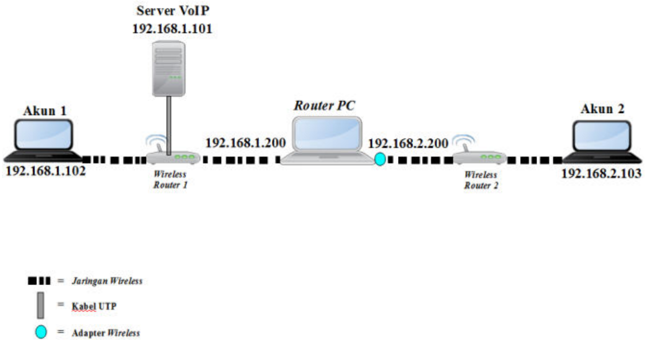


Fig 1. VoIP Network Topology Using WLAN

3. *Workload model*

This stage is determined by what it charges to the network researchers have created that. In this study, they charge two systems the VoIP system using WLAN and VoIP using WLAN.

4. *Simulates behavior under expected load*

This stage simulates a network system that has been determined at the workload model stage. At this stage, I also measure the Quality of Service against the VoIP system using WLAN.

5. *Do a sensitivity test*

At this stage, it implements the security system on a VoIP system using WLAN testing. The security used on this system is data encryption; the authors use Zfone software. Zfone uses the ZRTP protocol to encrypt data on the transport protocol used by the VoIP system using WLAN.

6. *Process design as needed*

At this stage, it results from the analysis carried out in the previous stages. The stage also redesigned if needed to get optimal results.

III. TESTING RESULTS

1. *Call flow process*

At this stage, we explain it about the process of a video call from the beginning of the video call until the end of the video call. Following result from testing the call flow process on a VoIPWLAN system without security and a VoIPWLAN system with Security:

a. *VoIP without security*

Following results from the process flow of the VoIPWLAN system without security presented in Figure 2.

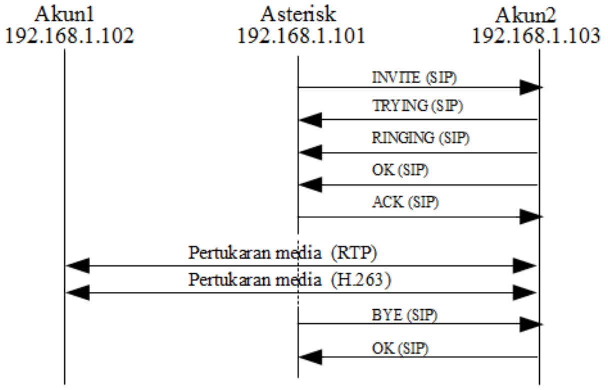
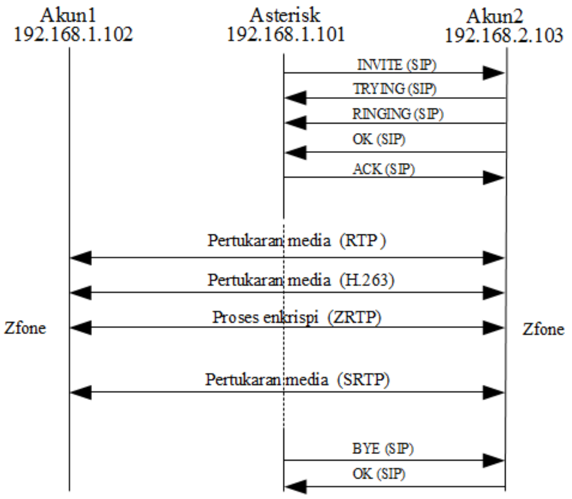


Fig 2. illustrates the process of initiating a video call flow

b. *VoIPWLAN with security*

The following result from the call flow process on the VoIPWLAN + ZRTP system presented in Figure 3.

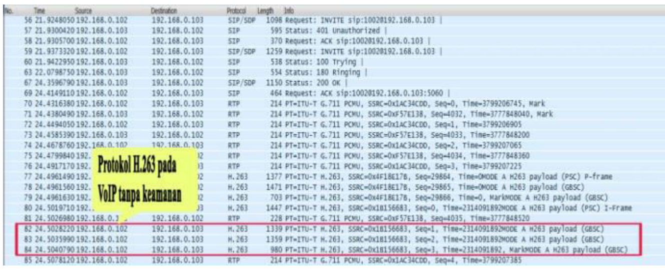


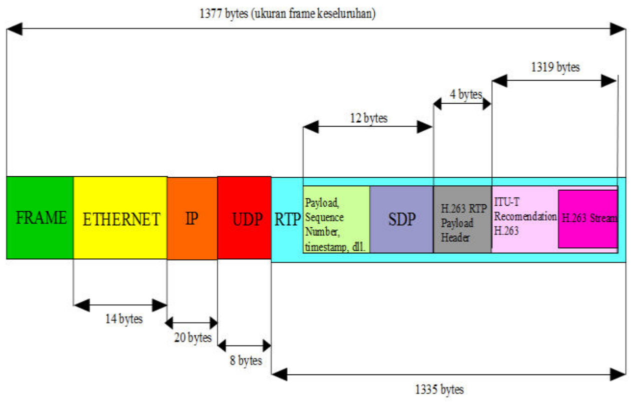
2. Transport protocol type

Based on the transport protocol used by the VoIPWLAN system before and after using security.

a. *VoIPWLAN without security*

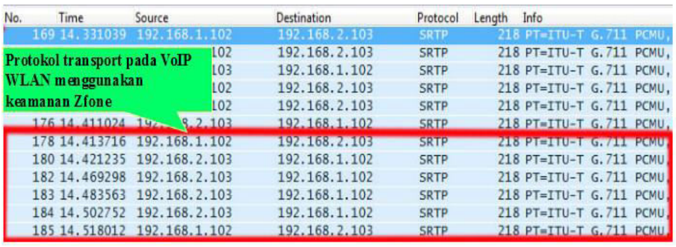
The following results of testing the transport protocol VoIPWLAN system without security, are presented in Figure 4 and we present the frame shape that carries the transport protocol in Figure 5.


```
No.  Time       Source        Destination   Protocol Length Info
56 21.9248050 192.168.0.102 192.168.0.103 SIP/SDP  1098 Request: INVITE sip:1002@192.168.0.103 |
57 21.9300420 192.168.0.103 192.168.0.102 SIP       595 Status: 401 Unauthorized |
58 21.9305700 192.168.0.102 192.168.0.103 SIP       370 Request: ACK sip:1002@192.168.0.103 |
59 21.9373320 192.168.0.102 192.168.0.103 SIP/SDP  1259 Request: INVITE sip:1002@192.168.0.103 |
60 21.9422950 192.168.0.103 192.168.0.102 SIP       538 Status: 100 Trying |
63 22.0798750 192.168.0.103 192.168.0.102 SIP       554 Status: 180 Ringing |
67 24.3596790 192.168.0.103 192.168.0.102 SIP/SDP  1150 Status: 200 OK |
69 24.4149110 192.168.0.102 192.168.0.103 SIP       464 Request: ACK sip:1002@192.168.0.103:5060 |
70 24.4316380 192.168.0.102 192.168.0.103 RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=0, Time=3799206745, Mark
71 24.4380490 192.168.0.103 192.168.0.102 RTP       214 PT=ITU-T G.711 PCMU, SSRC=0xF57E138, Seq=4032, Time=3777848040, Mark
72 24.4494050 192.168.0.102 192.168.0.103 RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=1, Time=3799206905
73 24.4585390 192.168.0.103 192.168.0.102 RTP       214 PT=ITU-T G.711 PCMU, SSRC=0xF57E138, Seq=4033, Time=3777848200
74 24.4678760 192.168.0.102 192.168.0.103 RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=2, Time=3799207065
75 24.4799840 192.                      2 RTP       214 PT=ITU-T G.711 PCMU, SSRC=0xF57E138, Seq=4034, Time=3777848360
76 24.4917170 192.                      3 RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=3, Time=3799207225
77 24.4961490 192.                      2 H.263    1377 PT=ITU-T H.263, SSRC=0x4F18E178, Seq=29864, Time=0MODE A H263 payload (PSC) P-frame
78 24.4961560 192.                      2 H.263    1471 PT=ITU-T H.263, SSRC=0x4F18E178, Seq=29865, Time=0MODE A H263 payload (GBSC)
79 24.4961630 192.                      2 H.263     703 PT=ITU-T H.263, SSRC=0x4F18E178, Seq=29866, Time=0, MarkMODE A H263 payload (GBSC)
80 24.5019710 192.                      3 H.263    1447 PT=ITU-T H.263, SSRC=0x18156683, Seq=0, Time=2314091892MODE A H263 payload (PSC) I-Frame
81 24.5026980 192.168.0.1   192.168.0.102 RTP       228 PT=ITU-T G.711 PCMU, SSRC=0xF57E138, Seq=4035, Time=3777848520
82 24.5028220 192.168.0.102 192.168.0.103 H.263    1339 PT=ITU-T H.263, SSRC=0x18156683, Seq=1, Time=2314091892MODE A H263 payload (GBSC)
83 24.5035990 192.168.0.102 192.168.0.103 H.263    1359 PT=ITU-T H.263, SSRC=0x18156683, Seq=2, Time=2314091892MODE A H263 payload (GBSC)
84 24.5040790 192.168.0.102 192.168.0.103 H.263     980 PT=ITU-T H.263, SSRC=0x18156683, Seq=3, Time=2314091892, MarkMODE A H263 payload (GBSC)
85 24.5078120 192.168.0.102 192.168.0.103 RTP       214 PT=ITU-T G.711 PCMU, SSRC=0x1AC34CDD, Seq=4, Time=3799207385
```



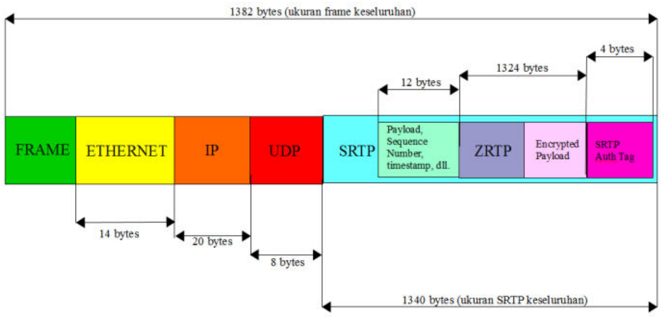
b. VoIPWLAN with security

The following results of testing the transport protocol, VoIPWLAN system with security, are presented in Figure 7 and I present the frame shape that carries the transport protocol in Figure 8.



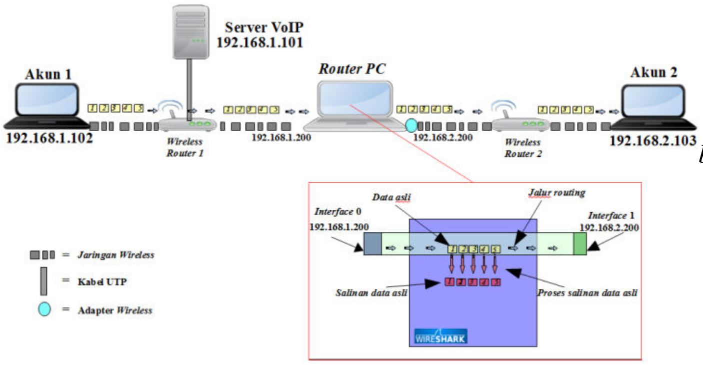
```
No.   Time       Source         Destination    Protocol  Length  Info
  169 14.331039  192.168.1.102  192.168.2.103  SRTP      218 PT=ITU-T G.711 PCMU,
                           102  192.168.2.103  SRTP      218 PT=ITU-T G.711 PCMU,
                           103  192.168.1.102  SRTP      218 PT=ITU-T G.711 PCMU,
                           102  192.168.2.103  SRTP      218 PT=ITU-T G.711 PCMU,
                           102  192.168.2.103  SRTP      218 PT=ITU-T G.711 PCMU,
  176 14.411024  192.    8.2.103  192.168.1.102  SRTP      218 PT=ITU-T G.711 PCMU,
  178 14.413716  192.168.1.102  192.168.2.103  SRTP      218 PT=ITU-T G.711 PCMU
  180 14.421235  192.168.2.103  192.168.1.102  SRTP      218 PT=ITU-T G.711 PCMU
  182 14.469298  192.168.2.103  192.168.1.102  SRTP      218 PT=ITU-T G.711 PCMU
  183 14.483563  192.168.2.103  192.168.1.102  SRTP      218 PT=ITU-T G.711 PCMU
  184 14.502752  192.168.2.103  192.168.1.102  SRTP      218 PT=ITU-T G.711 PCMU
  185 14.518012  192.168.1.102  192.168.2.103  SRTP      218 PT=ITU-T G.711 PCMU
```

Protokol transport pada VoIP WLAN menggunakan keamanan Zfone


1382 bytes (ukuran frame keseluruhan)
4 bytes
1324 bytes
12 bytes
FRAME
ETHERNET
IP
UDP
SRTP
Payload, Sequence Number, timestamp, dll.
ZRTP
Encrypted Payload
SRTP Auth Tag
14 bytes
20 bytes
8 bytes
1340 bytes (ukuran SRTP keseluruhan)

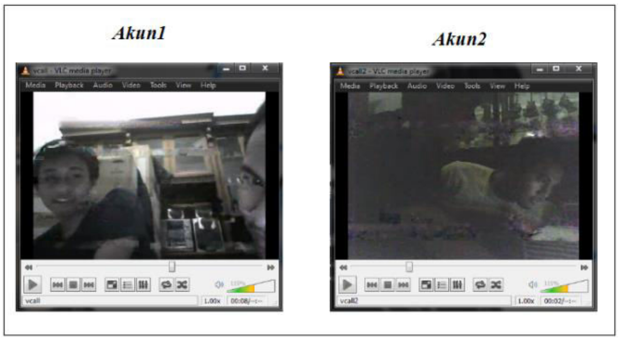
3. Video tapping results

Tapping is done by stealing data packets that become transport protocols on VoIP systems using WLAN. The transport protocol carries data that contains sound and image media that are generated from conversations conducted by the client. To do this, the writer uses Wireshark and PC router as the executor of tapping, as shown in Figure 9.



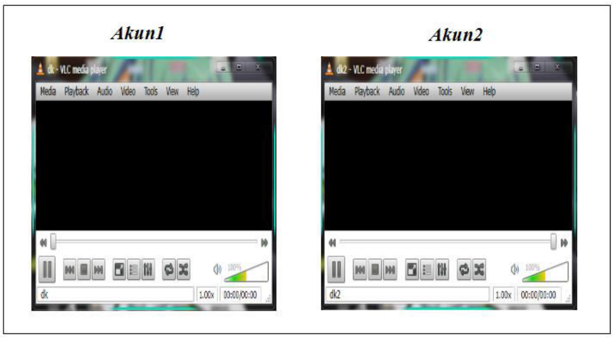
a. VoIPWLAN without security

Following result from tapping video calls on a VoIPWLAN system without security, presented in Figure 10.


Akun1
Akun2
vcall - VLC media player
vcall2 - VLC media player
Media Playback Audio Video Tools View Help

b. VoIPWLAN with ZRTP

The following result from tapping video calls on a VoIPWLAN system with security, presented in Figure 11.



4. Quality of Service Results

I carry quality of Service testing out five times, testing is done by making calls to account1 to account2. The parameters used are delay, jitter and packet loss. They carry the test out on a VoIPWLAN system without security and a VoIPWLAN system with security[1]

a. Delay

The following is the delay value in the VoIPWLAN system without security and with security, presented in table 1.

No	Testing	VoIPWLAN	VoIPWLAN+Zfone
1	Ke-1	72,59	78,77
2	Ke-2	74,07	81,48
3	Ke-3	100,7	83,64
4	Ke-4	71,73	73,41
5	Ke-5	25,58	83,29
Average		**68,93**	**80,12**

b. Jitter

Following is the value of jitter on a VoIPWLAN system without security and with security, presented in table 2.

No	Testing	VoIPWLAN	VoIPWLAN+Zfone
1	Ke-1	1,75	2,50
2	Ke-2	2,43	1,81
3	Ke-3	2,58	8,07
4	Ke-4	2,44	5,74
5	Ke-5	0,99	3,67
Average		**2,04**	**4,36**

c. Packet Loss

Following is the value of packet loss on a VoIPWLAN system without security and with security, presented in table 3.

No	Testing	VoIPWLAN	VoIPWLAN+Zfone
1	Ke-1	0	0
2	Ke-2	0	0
3	Ke-3	0	0
4	Ke-4	0	0
5	Ke-5	0	0
Average		**0**	**0**

CONCLUSIONS

Based on the research that has been done, the following conclusions can be drawn:

1. Zfone's security system affects securing video calls on WLAN. When video tapping is done, the ZRTP protocol turns the image of conversations between clients black.
2. The results of the quality of service before using the Zfone security system with the parameters of delay, jitter, and packet loss are as follows:
   a. The value of the delay time is 68.93ms
   b. The jitter time value is 2.04ms
   c. The packet loss parameter before using Zfone security is 0%.
3. The results of quality of service after using the Zfone security system with the parameters delay, jitter and packet loss are as follows:
   a. The value of the delay time is 80.12ms
   b. The jitter time value is 4.36ms
   c. The packet loss parameter after using Zfone security is 0%..

REFERENCES

[1] Solehudin, A., & Garno. (2017). PROTOTYPE API PADA APLIKASI PEMBATASAN AKSES INTERNET DENGAN PEMANFAATAN HAK AKSES USER PROFILE HOTSPOT. *Jurnal Rekayasa Informasi*, *19*(2), 16–25.

[2] Barrie Sosinsky Networking Bible. United States : Wiley Publishing, 2009

[3] CounterPath. 2006. *X-Lite* 3.0 *User Guide*. Diperoleh 10 Septermber 2013, dari http://www.counterpath.com/assets/files/191/XLite3.0_UserGuide.pdf

[4] Deris Setiawan, Fundamental Internetworking Development & Design Life Cycle. 2009.

[5] Gunadi Dwi Hantoro, Wifi (Wireless LAN) Jaringan Komputer Tanpa Kabel, Bandung, Informatika,2009.

[6] H. Schulzrinne, S. Casner, V. Jacobson. Network Working Group. Columbia University, 2003.

[7] Http://en.wikipedia.org/wiki/H.263. Diperoleh 21 maret 2014.

[8] Http://www.ebizzasia.com/0330-2005/focus,0330,03.htm. Diperoleh 19 april 2014.

[9] Kamaldila Puja Yusnika, IlmuKomputer.com, Model Referensi OSI. Diperoleh 5 mei 2014.

[10] Keith W. Ross, James F. Kurose. *Computer Networking : A Top-Down Approach (Sixth Edition)*. United States : Pearson Education. 2013.

[11] Matthew Gast *802.11 Wireless Networks The Definitive Guide*. United States : O'Reilly Media, 2005.

[12] Melwin Syafrizal, *Pengantar Jaringan Komputer,* Yogyakarta, Andi Publisher, 2005.

[13] Richard Sharpe, NS Computer Software and Services P/L Ed Warnicke, Wireshark User's Guide : for Wireshark 1.11. 2013.

[14] Richard A. Stanley, *Wireless LAN Risk and Vulnerabilities*. Diperoleh 13 Agustus 2013, dari http://kuainasi.ciens.ucv.ve/cisa/articles/v2-02p57- 61.pdf

[15] Rudi Hartono, S.Si & Agus Purnomo, S.Si, Wireless Network 802.11. D3 TI FMIPA UNS. 1/1/2011. Diperoleh 12 mei 2014.

[16] Sentot Kromodimoeljo, Teori dan Aplikasi Kriftografi. SPK IT Consulting. 2009.

[17] Samuel Stillo, Zfone : A New Approach for Securing VoIP Communication. 2006.

[18] T.J. Wals, D.R. Kuhn dan S.Fries, *Security Considerations for Voice over IP Systems*. United States : National Institute of Standards and Technology.2005.

[19] Wittenberg, *Voice over IP Technology*. Canada : Delmar Cengage Learning, 2009.