Implementation of VPN-SSL on OpenBTS as Data Security Transmitted between BTS and VoIP

Rino[1], Irfan Setiadi[2]
[1]Binus University, anakrangunpalsan@gmail.com
[2]Open University, irfaaniumuchem@gmail.com

ABSTRACT

OpenBTS is an open source software that utilizes a hardware device called USRP (Universal Software Radio Peripheral) as a transmitter and receiver of frequencies. OpenBTS also uses Asterisk's open source software for interconnection with other telephone networks such as PSTN (Public Switched Telephone Network) or other telecommunication operators using VoIP (Voice over IP). However in this communication there is a vulnerability to data transmitted between BTS via Ethernet.

The main objective of this research is to build GSM cellular networks using OpenBTS and USRP as a medium of information exchange in areas not yet covered by cellular services. In addition to provide communication security services, data transmitted will be secured using a VPN - SSL with SEED algorithm based on symmetric cryptography.

Keywords: Universal Software Radio Peripheral (USRP), SEED symmetric cryptographic algorithm, Global System for Mobile Communication (GSM), Base Transceiver Station (BTS), VPN-SSL.

1. Preliminary

1.1 Background

Mobile communication network is one of the services those are widely used for the exchange information on the mobile communication network mainly based on Global System for Mobile Communication (GSM). Almost all mobile communication developed at this time using GSM-based cellular communications network, because the network is a GSM mobile telecommunications network that has a standard architecture of the European Telecommunications Standards Institute (ETSI) [1]. Currently, GSM has become the global standard for communication, both in Indonesia and in the world [2].

In the exchange information is not easy when you're in an area that not yet covered by the BTS signal or can be called by blankspot area. To overcome these problems, one way to do that is, build Open Base Transceiver Station (OpenBTS) as a GSM-based mobile communication network to exchange information on blankspot area. In addition, this technology is so useful for building telecommunication networks in remote, rural, rural and disaster areas. Because if conventional BTS is built, the probability of tower success in these areas is so small and the required cost is quite large.

In the Fuadi's research in 2012, OpenBTS designed by implementing an asterisk in Ubuntu 10.10, you can use open source software that runs on Linux platform [11]. This OpenBTS Software utilizes Universal Software Radio Peripheral (USRP) as a medium to send and receive data via the GSM cellular. While OpenBTS will be investigated on this occasion there is a difference, namely the implementation of VPN-SSL using SEED algorithm on OpenBTS to secure data transmitted between BTS and VoIP. VPN-SSL implementation using SEED algorithm is aimed as security needs that can enable to obtain high level of strength and adequate speed in a network. [12]

1.2 Problem Formulation

The problem formulation in this research are:

1. Is the GSM-based mobile communication network using OpenBTS software can provide solution to blankspot area?

2. How to implement VPN-SSL on OpenBTS for communication between BTS and VoIP?
3. Is the VPN-SSL using SEED algorithm based symmetric cryptography can provide security service data transmitted between BTS and VoIP?

1.3 Objectives and Benefits of Research

In this study built GSM cellular communication system with OpenBTS as a solution to the blankspot area and carried VPN-SSL implementation on OpenBTS as a medium of exchange secure information on blankspot area as well as added security services on data transmission that is sent between BTS and VoIP. It is expected that this research can also enrich the library of education literature, as well as a reference in the field of security applications based on OpenBTS.

2. Theoritical Basis

2.1 GSM (*Global System for Mobile Communication*)

GSM (Global System for Mobile communication) is a technology used in communication with the digital systems and networks that has been already global. As a technology that can be said to be quite revolutionary because it successfully shifted the popular analog mobile telecommunication system technology in the decade of the 80s, GSM has provided a new communication alternative for the world of better telecommunication. By using a digital signal system in data transmission, the quality of data produced is better than analog system. In daily life we are more familiar with Handphone (HP) as the application of the most popular GSM technology. Since the first GSM implementation until now has been developed into three groups: the GSM 900, 1800 and 1900. The third difference is located based on group of frequency bands used. GSM 900 uses 900 MHz frequency as its transmission channel. GSM 1800 and 1900 each use the 1800 and 1900 MHz frequencies. Picture of GSM network architecture shown in Figure 1. [11]

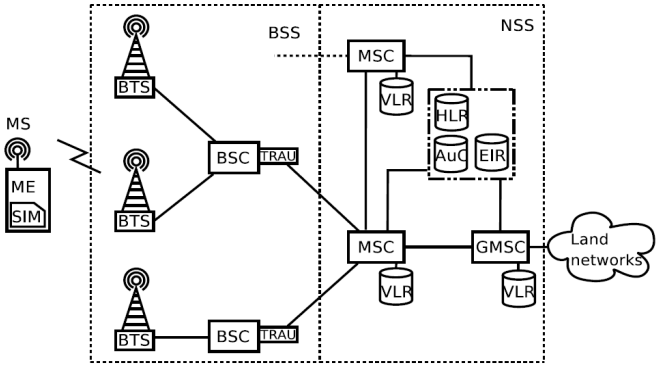

Figure 1. GSM network architecture

A GSM network is built of several functional components which have special function and interface. In general, GSM network divided into three main parts, namely:

1) *Mobile Station* (MS)

MS is a device used by customers to communicate. MS consists of Mobile Equipment (ME) and a Subscriber Identity Module (SIM).

- *Mobile Equipment* (ME) is a radio transmission terminal equipped with International Mobile Equipment Identity (IMEI), while the SIM provides the customer identification number to enter the GSM operator's network. ME serves as a transceiver (transmitter and receiver), as a transducer that converts sound signals into electric signals, monitor the condition of power and signal quality of the surrounding cells, and has a memory for storing user data.
- *Subscriber Identity Module* (SIM) has a microprocessor and a memory to store some users' data. Inside the SIM there are some important information that is used in communication such as the International Mobile Subscriber

Identity (IMSI), Authentication Key (consisting of algorithms A3 and A8) were used during the authentication process and it contains Personal Identification Number (PIN) and PIN Unblocking Key (PUK).

2) Base Station System (BSS)

BSS consists of three devices:

- *Base Transceiver Station (BTS)* is a transmitter and receiver device that handle radio access and interacts directly with MS through the air interface. BTS also sets the handover process that happens inside BTS and monitored by BSC.
- *Base Station Controller (BSC)* is the interface between the BTS to Mobile Switching Center (MSC) and Operation And Maintenance Center (OMC). BSC controls several BTSs and arranges traffic in and out from BSC to MSC or BTS. BSC sets of radio resource in the provision of frequency for each BTS and arranges handover when the MS crosses the line between cells.
- *Transcoder (XCDR)* serves to compress data or voice output from the MSC (64 Kbps) to 16 Kbps in the direction of the BSC and vice versa for the efficiency of the transmission channels.

3) *Network Switching System* (NSS)

NSS works as switch in a GSM network, sets the network, and becomes a media interface between the GSM network with other networks. NSS component on GSM network consists of:

- *Mobile Switching Center* (MSC), a network elements central in a GSM network. MSC as the core of the cellular network, where the MSC plays a role for interconnection of speech, either between cellular or with PSTN cable network, or with data network. MSC is responsible for managing communication between customers and other telecommunication network users.
- Home Location Register (HLR) is a database containing customer data remains an area of coverage. These data include customer services, additional service and information about the most recent customer location.
- Visitor Location Register (VLR) is a database that contains temporary information about subscribers who are roaming from another coveraged area.
- Authentication Center (AuC) contains confidential database that is stored in the form of a code format for securing and controlling the legal-based use of mobile systems and prevent customer fraud.
- Equipment Identity Register (EIR) is a centralized database that the function is to validate the International Mobile (IM).
- Inter Working Function (IWF) serves as an interface between a specific GSM network and other GSM networks.
- Echo Canceller (EC) is used as PSTN connector for reducing the echo and delay.

2.2 OpenBTS Architecture

OpenBTS is a prototype of GSM-based mobile communications network consisting of software and hardware. The software used can be downloaded for free like asterisk, GNURadio, etc. While the hardware used is the Universal Software Radio Peripheral (USRP). Both devices are what makes OpenBTS like a standard GSM mobile phone network. A software like asterisk is used to interconnect with other phone networks such as the Public Switched Telephone Network (PSTN) or other telecommunication operators by using Voice over IP (VoIP).[3] The OpenBTS architecture image is shown as in Figure 2. [1]

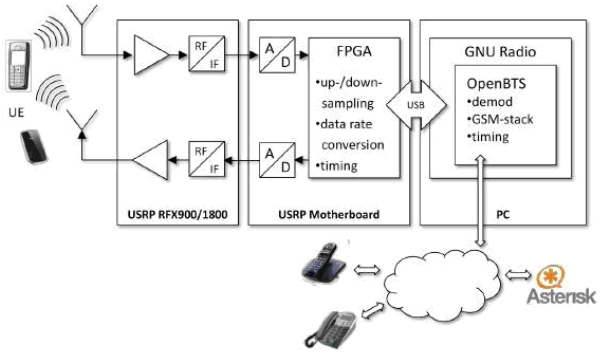

Figure 2. OpenBTS Architecture

1) Asterisk

Asterisk is an open source software that is usually used to build a system of communication services and provide more convenience for users to develop their own phone services with the broadest customization given to the user. From the definition of open source itself means that any developer can view and modify the source code available, so that existing applications can be added easily by any developer. Asterisk can also be regarded as a complete PBX in the form of software, and provides all the features like PBX. PBX (private branch exchange) is a telephone service provider that seves a telephone exchange with the center. [9]

2) Universal Software Radio Peripheral (USRP)

Universal Software Radio Peripheral (USRP) is a radio software based highly speed Digital Signal Processing (DSP). USRP is hardware and currently has several versions. The most recent version is using Gigabit Ethernet that can be stored above the tower easily so it can cover a wide area. [5]

3) GNU Radio

GNU Radio is one of the software that will be used in operating OpenBTS. GNU Radio is a set of device that provide signal processing. One of the advantage of GNU Radio is a software with open source code and free software. [5]

2.3 VPN (Virtual Private Network)

VPN or Virtual Private Network is a private connection via a public network or the Internet. Virtual network means the network must be characterized as virtual. Private mens nobody can access the network. The sent data will be encrypted so it remains confidential even though over a public network. Using VPN likes making a network inside network called by tunnel. VPN uses one of the three existing tunneling technology are: PPTP, L2TPand latest standards, Internet Protocol Security (commonly abbreviated as IPSec). VPN is a combination of tunneling and encryption technology.

How VPN works VPN (with the PPTP protocol) are:

- VPN requires a server to connect the PC, thisVPN server can be a computer with VPN application server or a router
- To start a connection, a computer with Client VPN application contacts the VPN server, VPN server then verifies the username and password, and if successful then the VPN Server delivers a new IP address on the client computer and then a connection / tunnel will be formed.
- Furthermore, the client computer can be used to access various resources (computer or LAN) located behind the VPN Server such as data transfer, document printing, browsing with the gateway provided from the VPN Server, remote desktop and so forth.

2.3.1 VPN Function

VPN technology provides three main functions for its users. The main functions are as follows:

- **Confidentiality**
  VPN technology has a working system to encrypt all the data passing through it. With this encryption technology, then your secrecy becomes more awake. Even if there are parties who can tap your data passing by, but not necessarily they can read it easily because it is already randomized. By implement-ing this encryption system, no one can access and read the contents of your data network easily.
- **Data Integrity**
  As it passes through the Internet network, your data has actually gone so far further across countries. In the middle of his journey, anything can happen to its content. Whether it is lost, damaged, even manipulated by bad person. VPN has technology that can keep the integrity of the data you send in order to arrive at its destination without being flawed, lost, corrupted, or manipulated by others.
- **Orign Authentication**
  VPN technology has the ability to authenticate the sources of data senders that will be received. VPN will check all incoming data and retrieve its data source information. Then the source address of this data will be approved if the authentication process succeeds. Thus, the VPN guarantees that all data sent and received by you, comes from the appropriate source. No data is forged or transmitted by other parties.

2.4 SSL (Secure Socket Layer)

According Stalling (2005), SSL is a tunneling layer transport protocol that is often used. SSL has several applications and can easily be used to build a tunnel layer transport. The protocol uses three cryptographic functions, namely:

1. **Key exchange**
   Both parties need a way to exchange keys. Part of the key exchange can provide the authentication process on the server.
2. **Data encryption**
   In this SSL there is a method for encrypting the data executed in this protocol. It uses symmetric algorithm, both stream and block ciphers.
3. **Authentication**
   In each transmitted record, it must be authenticated first. This can be done by adding a secret message of digest Hash Message Aunthentication Code (HMAC) for each record.

3. Research methodology

In this study the method used is qualitative. In qualitative research, the basic theory is used as a foothold or reference. This is done by means of techniques of data collecting, data analysis, system design, implementation, and testing.

The data used are descriptive, where the data can be photographs, documents, and field notes at the time of research is in progress. The technique used in qualitative method is observation technique, where the researcher is directly involved with the research. With the technique of document review, researchers will conduct a review of the documents.

3.1 Data Collection Technique

Data collection in this research is done by literature and interview technique. Literature technique is done by studying the theories related to research, such as SEED Algorithm-based symmetrical, Global System for Mobile Communication (GSM), Open Base Transceiver Station (OpenBTS), Virtual

Private Network (VPN), Secure Socket Layer (SSL), Wireshark, and others. In addition to studying the theory, literature technique is also done by studying the research or system ever made. The interview technique is done to the resource person, either directly or indirectly. By doing interview technique, it will get a lot of precise and accurate data.

3.2 Needs Analysis

After collecting the data, the results are used to determine what kind of system will be generated. In the need analysis phase, four objectives are achieved: to explain the complete system, to describe the system ideally, to bring the ideal system into the current state by paying attention to resource constraints, and confidence in the client about the system to be created. There are two kinds of needs found in this study, namely: functional and non-functional needs. The functional analysis is to define what should and can be done by the system ie, the system provides GSM-based communication services safely on the transmission conducted between BTS. Security used is with VPN-SSL. While the non-functional need analysis does not define what the system should do, but it is how the system does what it should and can do. For example, system performance, process or cryptographic scheme used, operational, security, and policies by IEEE, Cisco, and ITU.

3.3 System Planning

The system design will be made using the method of flowchart design. It is a method that is structured in the making. If the previous stage has not been completed, then the next stage can not be done, and the system built is not running. System design image created by using a flowchart shown in Figure 3.

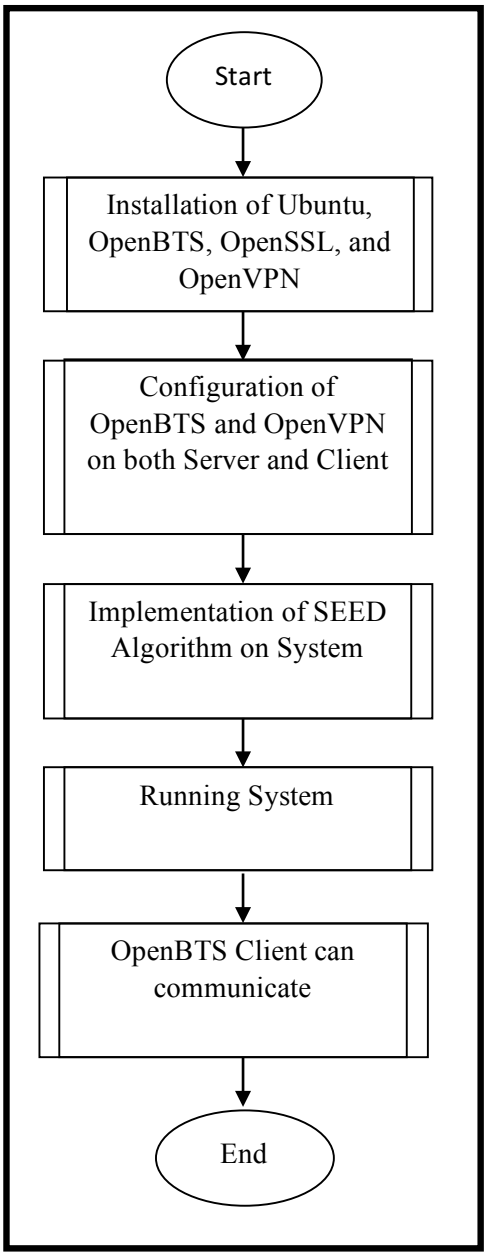

Figure 3. General System Design

3.4 Implementation

Implementation of this system begins with installing the required software such as, Ubuntu operating system, Asterisk, GNU Radio, OpenBTS, OpenVPN, and OpenSSL. Then continued with the configuration of the system that has been installed. After that compiling between OpenVPN and OpenSSL (VPN-SSL). Then the SEED algorithm in OpenSSL is implemented on this system with the aim of securing data on the transmission

between BTS and VoIP that exist in this system.

3.5 Testing

In this research, the system has been made was tested. The tests performed are as follows:

1. OpenBTS Parameter Measurement

   The purpose of this measurement is to determine the transmission quality of Mobile Station or GSM Handphome served OpenBTS when making phone calls. The transmission quality parameter analyzed are Rx level, Rx Quality, and SQI. The size of the transmission quality will provide information on whether the OpenBTS network implemented is feasible and meets the value of KPI (Key Performance Index) or not yet. While other parameters are BCCH and ARFCN to know the frequency used by OpenBTS. BCCH (broadcast control channel) itself is part of GSM channel control as the name implies is doing broadcasting of cell network data where the user is located and what the neighbour cells. While ARFCN is the code that defines a pair of radio and channel carriers that are used for transmitters and receivers in the Um interface, one for uplink signals and one for downlink signals.
2. Measurement of QoS (Quality of Service)

   Measurement of Quality of Service (QoS) aims to measure parameters that support the quality of OpenBTS and VoIP. The measured parameters include delay, jitter, throughput, and packetloss. The parameter values obtained are compared with the existing QoS standard values, whether they are within predetermined standards or not. Meanwhile, to get the values of the QoS parameters itself used Wireshark as a network protocol analyzer. As a value reference of QoS parameters obtained, then the standards of some institutions served as a reference, among others:

   a. Jitter is considered good-value <50 ms (ITU-T G.1010), and is worth <30 ms (Cisco)
   b. The best delay value between 0-150 ms (ITU-T standard)
   c. Packetloss considered good if the value of <1% (ITU-T standard)
3. CPU Usage Measurements

   Measuring performance of Asterisk server by paying attention on the CPU Usage at Asterisk server when communication occurs on the client asterisk. There are three scenarios of communication made at the time of measurement, namely, VoIP to VoIP, OpenBTS to VoIP, and OpenBTS to OpenBTS, so we can determine how much CPU Usage amount used in these three processes. Going forward, there will be an estimated number of users that can be handled by the server at a time.
4. Testing Data Traffic Security

   Knowing and proving the performance of VPN-SSL by capturing data packet transmitted to the server when communication occurs on the client. There are three scenarios of communication made at the time of measurement, namely, VoIP to VoIP, OpenBTS to VoIP, and OpenBTS to OpenBTS, so it can be known whether data packet transmitted over VPN-SSL tunnel was encrypted or not when these three processes were done. Going forward, it can be predicted whether securing using VPN-SSL with symmetric-based SEED algorithms is effective and feasible to use or not.

3.6 Analysis

Analysis was based on the analysis from the results of the implementation of a mobile communication system that is built, the analysis of data security, performance analysis and analysis of system deficiencies. In the data security analysis, analysis is conducted based on the results of the testing process. While the analysis of system deficiencies is an analysis from the lack of systems that still need improvement or further research. Moreover, there was also conducted

analysis of performance testing results where the system is built to know how strong the performance is owned.

4. Design and Implementation

Here is the OpenBTS system design in this research.

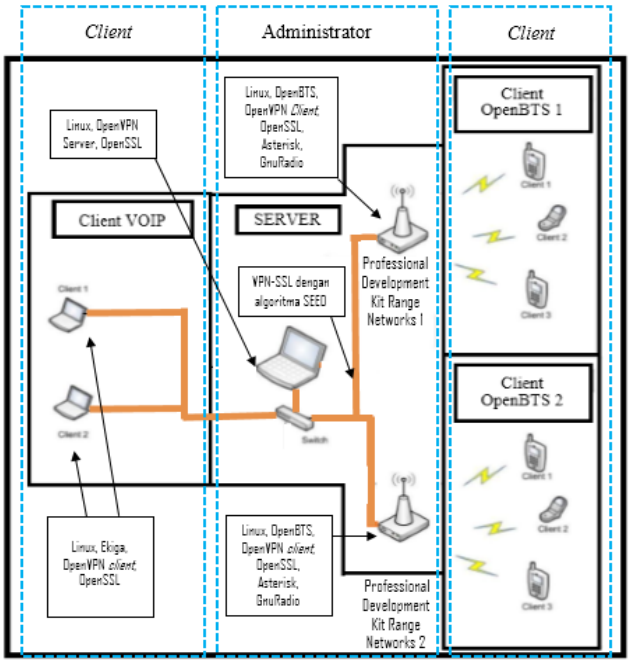

Figure 4. System Design

From the picture above, system design is divided into several parts, namely:

- OpenBTS Client
  OpenBTS Client is a form of mobile device that is used as the MS to connect the communication between Professional Development Kit Range Networks with the server and serves as a transceiver terminal (transmitter and receiver signal) to communicate. While simcard in MS will serve to provide information on the number of International Mobile Subscriber Identity (IMSI) which can be recognized by the OpenBTS network.
- VOIP client
  VOIP client is a laptop device with software telephone in this case using Ekiga application used as a client that can be connected to the OpenBTS network using or past an IP network. This is done because they want to connect/interconnect to external network and this client can be regarded as a gateway.
- Server
  Server consists of a laptop and a Professional Development Kit Range Networks. Laptop are only used to control whether Professional Development Kit Range Networks 2 as the management of information data center information or as the Home Location Register, the running system control and user registration management well. Professional Develop-ment Kit Range Networks is a replacement from the Base Transceiver Station (BTS) which is served as a sender and recipient from emitted network signal. There are several programs and supporting applications that needed to be installed as well, such as: Asterisk, GNU Radio, OpenBTS, MySQL Server, Smqueue.

5. Testing and Analysis Results

To verify the VPN capabilities which is implemented in this OpenBTS system, some tests are performed. Tests were done is Quality of Service (QoS) and data traffic security testing. From the test results obtained, are presented in the table below:

TABLE 1. OF QUALITY OF SERVICE RESULTS

No	Parameter	Result
1	Delay	• OpenBTS to VoIP = 19.98ms • VoIP to Voip = 19.99ms • Delay < 150ms (Good by ITU)
2	Jitter	• OpenBTS to VoIP = 0.82ms • VoIP to Voip = 0.92ms • Jitter is said to be good, if < 50ms by cisco and < 30ms by ITU

3	Packetloss	• OpenBTS to VoIP = 0% • VoIP to Voip = 0% • Package Loss is said to be well interrupted < 1 % by ITU
4	Throughput	The more dense the background traffic on the network will be, the less successful number of bits sent, measured in bytes per second

From the results captured using Wireshark, it can be shown that the application used is the UDP protocol with OpenVPN port. Figure 5 shown the results of SMS communication, the use of OpenVPN port is indicated by red striped box.

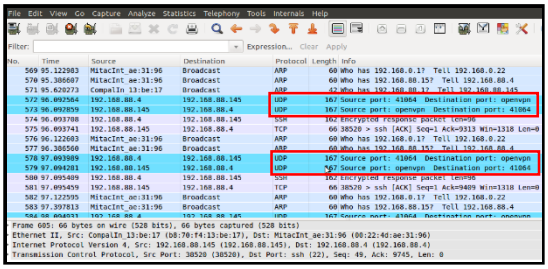

Figure 5. Results Captured from SMS Communication

Otherwise, when communicating by phone, the use of OpenVPN port is shown in picture 6 premises red striped box as well.

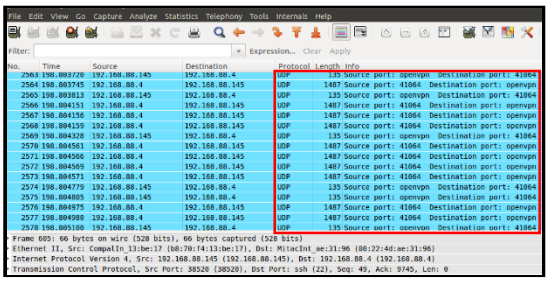

Figure 6. Results Captured from Communication

To see more details, then seen the results of encryption that has been done with OpenVPN, in Figure 7 is a packet of data encrypted with SEED algorithm, the encrypted message is meaningless.

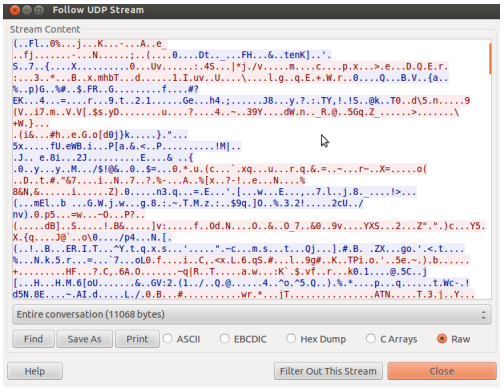

Figure 7. Encrypted Data Packet Content

From the three images above, it appears that the path used is a preconfigured OpenVPN port. The path uses symmetric-based SEED algorithm encryption for communication of the three determined scenarios, the client OpenBTS to OpenBTS, OpenBTS to VoIP and VoIP to VoIP.

6. Cover

6.1 Conclusion

Based on the results tests of the implementation, process, and analysis, it can be concluded as follows:

1. GSM-based mobile communication network by using OpenBTS software can be used on a local blankspot area.
2. Safeguarding the transmission of data via Ethernet using VPN-SSL with symmetric-based SEED algorithm can be implemented well. All of the data transmitted via VPN-SSL tunnel are encrypted first. To sum up VPN-SSL can be implemented as additional security during data transmission over Ethernet.
3. parameters testing associated with OpenBTS transmission analysis by using walktest test through Terms Investigation Software conducted by two scenarios shows that the OpenBTS network communication link is feasible despite the reach is small. The resulting value is Rx average level of -55 dBm, Rx Quality average of 1.17, and the average SQI is 13:59.
4. QoS measurement result indicates that the VoIP network connected with OpenBTS meets VoIP QoS standard

(Delay = <50ms, Jitter = <15ms and Packet Loss = <1%).

5. CPU Usage measured on the server generates 1-2% increase for VoIP to VoIP, for VoIP communication to OpenBTS increase as much as 4-5%, while for OpenBTS to OpenBTS increase 6-7%. To achieve more CPU Usage (95-100%) the estimated number of OpenBTS client to OpenBTS that can be served is approximately 12 clients that communicate at the same time.

Reference

[1] Azad, Abul. (2013). OpenBTS Implementation With Universal Software Radio Peripheral.

[2] Kemetmuller, C. (2010). Installation Guide for OpenBTS. Darmstadt: CASED

[3] David A. Burgess, Harvind S. Samra. 2008. The OpenBTS Project. Kestrel Signal Processing, Inc. Fairfield, California.

[4] Kanaiya Kanzaria, sanjay s.c. (2014). Active GSM Monitoring.

[5] Desai Karan, Ravikiran Dinakar. (2010). Licensing and Security Issues in the Implementation of OpenBTS Base GSM System.

[6] Fabian V.D.B. (2010). Catching and Understanding GSM-Signal.

[7] KISA. SEED Algorithm Specification.

[8] NIST SP.800-113. (2008). Guide to SSL VPNs.

[9] ITU-T P.800. (1996). Methods for Subjective determination of transmission quality.

[10] RFC5669 (2010). The SEED Cipher Algorithm and Its Use with the Secure Real-Time Transport Protocol.

[11] Fuadi, H., 2012. *Perancangan dan Implementasi OpenBTS dengan Menggunakan Asterisk di Ubuntu 10.10.* s.l.:s.n

[12] Hosner, C., 2004. OpenVPN and the SSL VPN Revolution. Volume GSEC v.1.4b.