Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2016, 3(2):47-51**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

TCP Packet Steganography using SDA Algorithm

Rajib Biswas[1], Samir Kumar Bandhyapadhyay[2]

[1]Department of Information Technology, Heritage Institute of Technology, Kolkata.
[2]Department of Computer Science and Engineering, Calcutta University, Kolkata.

Abstract This electronic document represents the comparative study of transmission of encrypted data packet using different cryptographic algorithm.

Keywords Cryptography, WLAN, Network Steganography

Introduction

Exchange, production and storage of information is becoming more and more substantial in the functioning of societies, hence the task of securing the information from unwanted and unsought use becomes more complex. Our aim is to provide confidentiality in the communication of digital information and distinguish a subset of such procedures called *Network Steganography* [1] which is a technique of information hiding that utilizes network protocols as enablers of hidden communication.

Cryptography [2] protects messages from being captured by unauthorized parties while Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography.

With the latest advancements, the constraints on the message length have been removed. Such methods are harder to detect and eliminate. Thus steganography provides not only security, but also privacy. In today's world the mule that co-conspirators are using is not the carrier itself but the communication protocols that govern the carrier's path through the Internet.

Network Steganography covers a broad spectrum of techniques, which include, among others:

Steganophony - The concealment of messages in Voice-over-IP conversations, alternatively, hiding information in unused header fields is streganophony [3].

WLAN Steganography - Transmission of steganograms in Wireless Local Area Networks. A real world application of WLAN Steganography is the HICCUPS system (Hidden Communication System for Corrupted Networks) [4].

Literature Review

VoIP steganography [3] is a real-time network steganography, which utilizes VoIP protocols and traffic as a covert channel to conceal secret messages. Recently, there has been a noticeable increase in the interest in VoIP steganography due to the volume of VoIP traffic generated, which proved to be economically feasible to utilize.

Krzystof Szczypiorski put forward HICCUPS (HIdden Communication system for CorrUPted networkS) [4], a steganographic system dedicated to shared medium networks including wireless local area networks. The novelty of HICCUPS is: usage of secure telecommunications network armed with cryptographic mechanisms to provide steganographic system and proposal of new protocol with bandwidth allocation based on corrupted frames.

In the work by Józef Lubacz *et al* [5], a comparatively new research is presented in the subject in the area of information hiding is presented, followed by a concise overview and classification of network steganographic methods and techniques.

Hiding information in network traffic may lead to leakage of confidential information. Bartosz Jankowski *et al* introduce a new steganographic system: the PadSteg (Padding Steganography) [6]. It is an information hiding solution which represents inter protocol steganography i.e. usage of relation between two or more protocols

from the TCP/IP stack to enable secret communication.
Wojciech Mazurczyk et al have presented a new steganographic method for IP telephony called TranSteg (Transcoding Steganography) [7]. Typically, in steganographic communication it is advised for covert data to be compressed in order to limit its size. In TranSteg it is the overt data that is compressed to make space for the steganogram.
In the work of Wojciech Mazurczyk and Krzysztof Szczypiorski [8] various steganographic techniques that can be used for creating covert channels for VoIP (Voice over Internet Protocol) streams are dealt with. Apart from characterizing existing steganographic methods we provide new insights by presenting two new techniques. The first one is network steganography solution which exploits free/unused protocols‟ fields and is known for IP,
UDP or TCP protocols but has never been applied to RTP (Real-Time Transport Protocol) and RTCP (Real-Time Control Protocol) which are characteristic for VoIP. The second method, called LACK (Lost Audio Packets Steganography), provides hybrid storage-timing covert channel by utilizing delayed audio packets. The results of the experiment, that was performed to estimate a total amount of data that can be covertly transferred during typical VoIP conversation phase, regardless of steganalysis, are also included in this paper.
Miłosz Smolarczyk et al have published a new steganographic method called RSTEG (Retransmission Steganography) in their paper [9], which is intended for a broad class of protocols that utilizes retransmission mechanisms. The main innovation of RSTEG is to not acknowledge a successfully received packet in order to intentionally invoke retransmission. The retransmitted packet carries a steganogram instead of user data in the payload field.
Professor KC Chen worked on the principles of network security [10] that would be possibly applied in wireless broadband networks are introduced. Widely applied digital encryption standard (DES) and recent advanced encryption standard (AES) are described due to their roles in networking environments.
Kamran Ahsana [11] investigated the existence of covert channels in computer networks by analyzing the transport and the Internet layers of the TCP/IP protocol suite. Two approaches for data hiding are identified: packet header manipulation and packet sorting. Each scenario facilitates the interaction of steganographic principles with the existing network security environment.
The typical steganographic method [12] introduced by Nitin Malik utilizes digitized media files (images, video and audio files) as a cover medium for hiding data, network steganography uses communication protocols such as TCP/IP. Such methods make it harder to detect and eliminate.

Experimental Work
Now there are two ways of implementing this method to achieve network steganography-

A. The first way is encrypting the data part and sending the key through the sequence number.
B. The second way is encrypting the sequence no. before sending the custom data packet.

The first method is used when symmetric key cryptography is used. Here the key exchange is a problem as the sender and receiver must use the same key to encrypt and/or decrypt. This method tries to eliminate the problem of key exchange a little bit. The steps followed are:

- Encryption and sending of the packet:

At the first step the cryptographic algorithm RSA/DES is run on a plain text to obtain the cipher text. Then a customized packet is created with the “data” field containing the cipher text obtained from the RSA/DES algorithm, and the 32 bit “sequence number” field containing the key to decrypt the cipher text. The customized packet is then sent to the receiver.

- Receiving of the packet and decryption:

This is basically the reverse operation of the previous step. A network analyzing tool such as Wireshark [15] is needed to be installed in the receiver’s computer to analyze the capture the packet sent from the sender. The receiver after receiving the packet first checks the “data” field to obtain the cipher text. Then the key to decrypt the cipher text is extracted from the 32 bit “sequence number” field. Finally the cryptographic algorithm RSA/DES is run on the cipher text using the key to obtain the plain text.
Comparative study between RSA & DES algorithm is done for encrypted packet sending efficiency in these 2 cases explained below.

A. Sda Algorithm:
1. SDA ALGORITHM FOR SENDING CUSTOMISED PACKETS (SDAPS)
Step 1: Start
Step 2: Read number of packets to send
Step 3: Create customized TCP/IP packets
Step 4: Set “SEQUENCE NUMBER‟ =‟e‟ (*obtained from RSA*)
Step 5: Set “DATA‟ =‟Cipher Text‟ (*obtained from RSA*)
Step 6: Initiate counter equal to one

Step 7: If counter less than no. of packets to be sent
Then
Step 7.1: Send packet
Step 7.2: increment counter by one
Step 7.3: go to step 7
Step 8: End
2. SDA ALGORITHM FOR RECEIVING CUSTOMISED PACKETS & DECRYPTING (SDAPR)
Step 1: Start
Step 2: Open WIRESHARK terminal
Step 3: Start capturing TCP packets from sender's computer
Step 4: SET "Cipher text"= value of "data" field from the captured TCP packet
Step 5: SET "e"= value of "Seq No." field from the captured TCP packet
Step 6: CALL RSA/DES function,
Step 7: DECRYPT "Cipher Text" To obtain "Plain Text" using the value of "e"
Step 8: End

Results and Discussion

For the accomplishment of this project the operating platform used is Ubuntu 14.04. The programs have been developed in C and compiled in open source OS terminal.
We performed 3 operations with parameters like sequence no., data field & a combination of both. They are defined as follows:

- Operation 1:

In this case the encrypted data is sent through only the sequence number field of the TCP packet. So the receiver has to extract the sequence number field of the captured packet and use the decryption part of the RSA/DES algorithm to obtain the plain text.

- Operation 2:

In this case the encrypted data is sent through only the data field of the TCP packet. So the receiver has to extract the data field of the captured packet and use the decryption part of the RSA/DES algorithm on it to obtain the plain text.

Table 1: Des Algorithm

No. of packets sent	No. of packets received	No. of packets dropped	Time Taken (sec)	% packets successfully delivered
10000	9514	486	3	95.14%
20000	18912	1088	5	94.56%
30000	28131	1869	7	93.77%
40000	37164	2836	8	92.91%
50000	46085	3915	9	92.17%
60000	54864	5136	11	91.44%
70000	63511	6489	13	90.73%
80000	71960	8040	15	89.95%
90000	80271	9729	16	89.19%
100000	88236	11764	17	88.23%

The table shows a detailed analysis of the number of packets sent to the receiver, the number of packets successfully captured by the receiver and the successful packet transmission rate.
The following bar chart and graph analyses graphically the number of packets sent to the receiver, the number of packets received and that of packets dropped by the receiver for the first case.

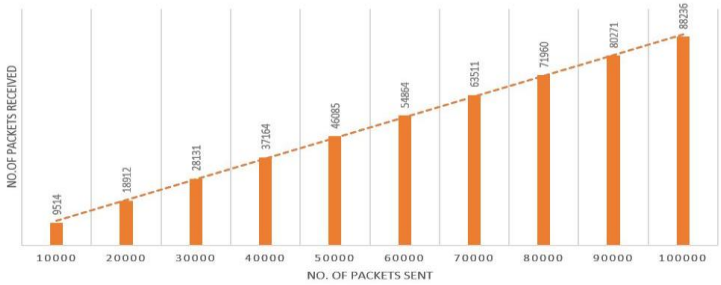

Figure 1: Result analysis bar chart of DES ALGORITHM

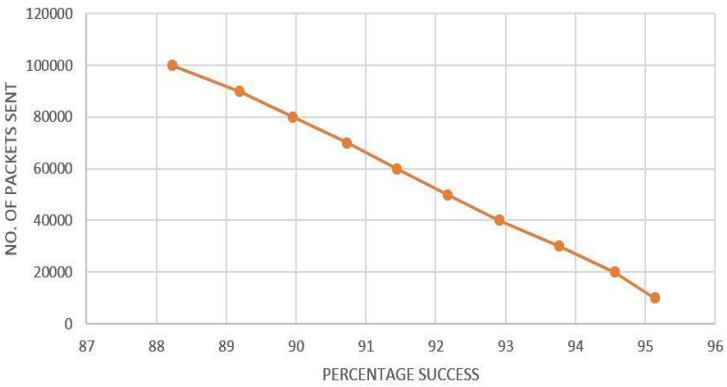

Figure 2: Result analysis graph of DES Algorithm

Table 2: Rsa Algorithm

No. of packets sent	No. of packets received	No. of packets dropped	Time Taken (sec)	% packets successfully delivered
10000	9875	125	4	98.75
20000	19650	350	5	98.25
30000	29001	999	6	96.97
40000	38344	1656	8	95.86
50000	47540	2460	9	95.08
60000	56286	3714	10	93.81
70000	65499	4501	13	93.57
80000	73992	6008	15	92.49
90000	81873	9127	16	90.97
100000	90591	9409	17	90.59

The table shows a detailed analysis of the number of packets sent to the receiver, the number of packets successfully captured by the receiver and the successful packet transmission rate.
The following bar chart and graph analyses graphically the number of packets sent to the receiver, the number of packets received and that of packets dropped by the receiver for the second case.

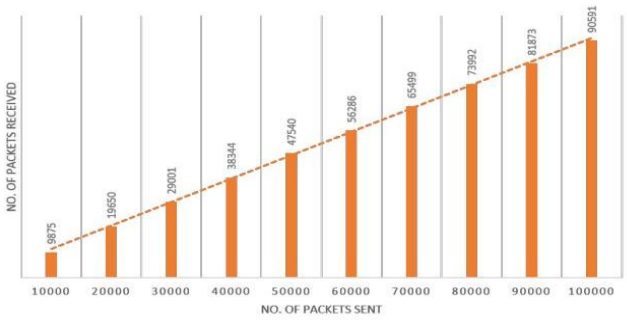

Figure 3: Result analysis bar chart of RSA Algorithm

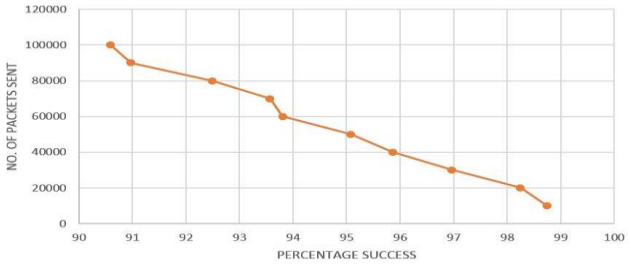

Figure 4: Result analysis graph of RSA Algorithm

Conclusion & Future Scope

The work that is done here on Network Steganography is one of its many applications. The data that is qualified as sensitive is passed through the sequence no. in an encrypted form which the receiver decrypts when the packet reaches his computer using RSA & DES algorithm.

The whole process is carried out with the help of a software called Wireshark. Wireshark is implemented using programs. In our study we took help of another software called Network Simulator to run it in a simulated environment before running in an actual environment.

Network Simulator makes use of packages which is why it's different from Wireshark.

Thus we reach to the successful execution and completion of the project using these softwares.

No technology or project work is perfect, it has to be developed further to make it perfect. Our project is also not an exception to that.

The main concern in our project is the number of Packets that get dropped during transmission from source node to the receiving node. The number of packets dropped can be decreased and this project can be perfected in future using newer technologies and exploring further in the field of Network Steganography.

References

[1]. FrączekWojciech, Mazurczyk Wojciech & Szczypiorski Krzysztof. (2011).How Hidden Can Be Even More Hidden, IEEE International Conference on Multimedia Information Networking and Security.

[2]. MeyerCarl H. &Matyas Stephen M (1982). Cryptography: A New Dimension in Computer Data Security, John Wiley & Sons, New York.

[3]. 2011 Fifth International Conference on Secure Software Integration and Reliability Improvement ReLACK: A Reliable VoIP Steganography Approach Mohammad Hamdaqa, Ladan Tahvildari Software Technologies Applied Research (STAR) Group, Department of Electrical and Computer Engineering University of Waterloo, Waterloo, Canada {mhamdaqa, ltahvild}@uwaterloo.ca.

[4]. SzczypiorskiKrzystof (2012).HICCUPS: Hidden Communication System for Corrupted Networks Warsaw University of Technology, Institute of Telecommunications ul. Nowowiejska , Warsaw, Poland.

[5]. LubaczJózef, MazurczykWojciech&SzczypiorskiKrzysztof (2012).Principles and Overview of Network Steganography, Institute of Telecommunications, Warsaw University of Technology, Warsaw, Poland .

[6]. JankowskiPadding Bartosz, MazurczykWojciech&Szczypiorski Krzysztof (2015).Information Hiding Using Improper Frame, Institute of Telecommunications, Warsaw University of Technology, Nowowiejska, Warsaw, Poland.

[7]. MazurczykWojciech,PawełSzaga& SzczypiorskiKrzysztof(2011).Using Transcoding for Hidden Communication in IPTelephony Warsaw University of Technology, Institute of Telecommunications Warsaw, Poland.

[8]. MazurczykWojciech & SzczypiorskiKrzysztof (2015). Steganography of VoIP Streams Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications, Warsaw, Poland.

[9]. MazurczykWojciech, SmolarczykMiłosz, SzczypiorskiKrzysztof(2009).Retransmission steganography and its detection, Springer-Verlag .

[10]. Professor ChenKC .Network Security &Steganography, Institute of CommunicationEngineering & Department of electrical Engineering, National Taiwan University.

[11]. AhsanaKamran (2012).Covert Channel Analysis and Data Hiding in TCP/IP ,Department of Electrical and Computer Engineering University of Toronto.

[12]. Rana Joshi .Network-based Steganography using Encryption in TCP/IP Header,ITM University Gurgaon.

[13]. JamgekarRajan.S.&JoshiGeeta Shantanu(2013). File Encryption and Decryption Using Secure RSA, International Journal of Emerging Science and Engineering (IJESE)

[14]. BellowinS.M. AT&T Bell Laboratories Murray Hill,New Jersey. Security Problems in the TCP/IP Protocol Suite.

[15]. https://www.wireshark.org