Efficiently Secure Data Communications Based on CBC-RC6 and the Overflow Field of Timestamp Option in an IPv4 Packet

Wid Akeel Awadh, Ali Salah Alasady and Alaa Khalaf Hamoud
E-mail: wid.jawad@uobasrah.edu.iq, ali_s.hashim@uobasrah.edu.iq, alaa.hamoud@uobasrah.edu.iq
College of Computer Science and Information Technology, University of Basrah, Iraq

Keywords: cryptography, network steganography, TCP/IP, IPv4, timestamp option

Received: February 14, 2022

In recent times, many researchers have directed their research efforts toward increasing the privacy and security requirements in the wireless communication networks area. The reason for this is the inappropriateness of using traditional security processes for reliable, efficient, and robust communication over networks that are not secured. Thus, this study contributes to the enhancement of security in wireless communication networks by proposing the use of steganography combined with cryptography so that secret information can be sent using IPv4 as a cover to conceal secret messages, thereby, securing the messages. Steganography is described as the process of concealing secret data in a way that it cannot be traced by an intruder. Here, the intruder is unable to detect any modifications made to the original media. Meanwhile, cryptography is referred to as the process through which plain text can be converted into ciphertext to enable the transmission of data through certain channels of communication in a format that cannot be read by a normal user. Network Steganography is a mechanism that involves the use of protocols for communication that control the path of the channel via the network. Initially, the TCP/IP protocols have been a good candidate for network steganography, due to the many benefits that can be derived from their use. One of such benefits is that allows the creation of a variety of concealed channels that can be used for secret communication. In order to enable communication over the network, the use of Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) is employed in the proposed system so that the encryption/decryption key can be generated. The initial step in our study involves encrypting the secret data that needs to be protected, and this is achieved through the use of the CBC-RC6 cryptographic algorithm. After the encryption has been successfully performed, a covert channel is created for the encrypted data through the use of the Overflow field of the Timestamp option of IPv4. With this method, debugging and measurement over networks are carried out using the timestamp option, and the aim of this is to build storage-based network steganography. One of the strategies used in this work to deter the possible detection of covert communication is the deployment of legal overflow data.

Povzetek: Opisana je metoda učinkovitega varnega prenosa podatkov na osnovi CBC-RC6.

1 Introduction

Recently, different spheres of life have witnessed the unavoidable role played by information security in our daily endeavors. More so, the increase in the use of digital communications has been recorded as a result of the increased use of mobiles, computers, and communication technologies. Thus, the emergence of digital communications has been witnessed by almost all sectors of life including military, training, e-commerce, e-learning, e-health, etc. [1, 2]. All these developments have resulted in the daily transmission of a large amount of data through the use of shared public networks, particularly the web. Therefore, secured and private communications are required by users so that their secret data can be protected from the activities of hackers, especially when the message is sent over an open channel [3].

Steganography and Cryptography are two methods with high interactivity which can be used in achieving secure communication. However, when they are used separately their effectiveness may be lower than when they are used together. In other words, cryptography or steganography may not be robust enough to protect secret data [4-7]. Hence, in this study, the two methods have been combined in an attempt to improve the security level of secret data, while maintaining the privacy and secrecy of data. These two methods have a unique way of providing security for information, but in order to achieve multiple layers of security, combining both methods is recommended [8].

In terms of achieving information security, steganography and cryptography are regarded as the most relevant methods that can be used [9]. Cryptography provides security for data by altering the secret information, such that, it cannot be read by intruders, but this is not the case with steganography as it is impossible for the unauthorized entity to detect the presence of the information, because it is totally hidden [10, 11].

When steganography is used in securing information, the information is embedded within digital media such as video, audio, document, or even a network protocol as a cover object [12]. This area of research has witnessed the emergence of a new field, which is referred to as network steganography, which allows the usage of Protocol Data Units (PDUs) as cover for the concealed data with alterations in fields that are unnecessary of the particular PDU concealed data; this is a unique attribute of the network steganography which is not obtainable with other methods of steganography. For example, one of the setbacks of the other techniques is that extra bandwidth is required to send the cover media with hidden data. Researchers in this emerging area of network steganography have proposed the use of popular protocols for the implementation of network steganography. It is only through the use of this technique that secret information can be hidden within the network protocols' payload or header or both. More so, it is able to provide sufficient bandwidth for secret data communication, because new data packets can be created for the conveyance of secret information, or even make alterations to extant packets to convey covert data [13].

This paper focuses on the concept of combining cryptography and steganography so that improved security and privacy can be achieved. In this work, these two methods are applied concurrently and after that, they are merged straight away, so the original message cannot be detected by the intruder. Thus, these two methods are applied concurrently with higher levels of security, so that a well-secured system for data hiding can be achieved.

In the proposed system, the use of a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) was employed in generating the encryption/decryption key. With the CBC-RC6 Algorithm, the secret text can be encrypted, and afterward, a concealed channel is created through the use of the timestamp function of Internet Protocol version 4 (IPv4). The concealed communication is implemented using Transmission Control Protocol (TCP) as a reliable transport layer protocol. In the TCP segment, transmission is enabled by using the underlying IP at the network layer. It is at this point that a covert channel is created through the use of the Overflow field of the timestamp option in the IPv4 header. The experimentation and implementation of the scheme are done over a Local Area Network (LAN).

2 System Overview

2.1 Cryptography

Cryptography refers to the science which is concerned with the concealing of information with the aim of keeping it away from intruders [14]. Previously, this science only revolved around decryption and encryption of messages that were exchanged through the use of secret keys, however, in recent times, there are different methods that are currently in use, including, Hashing, Asymmetric Key Encryption, and Symmetric Key Encryption [4, 15]. Normally, the information that needs to be concealed is referred to as "Plain Text", and the process of concealing the information is known as "encryption". The original text which is encrypted is referred to as "Cipher Text", while the term "Encryption Algorithm" refers to the set of rules employed during the encryption of the original text. Typically, the "encryption key" plays a crucial role in the process of encryption; this is because it is the input to the message and algorithm [16]. In cryptography, the retrieval of information from the encrypted text cannot be achieved without the use of a "decryption algorithm" which makes use of an appropriate "decryption key" to extract plain text [17, 18]. Every encryption system has particular security conditions guiding its operation including, integrity, authentication, confidentiality, and privacy [19].

2.2 Network Steganography

Network steganography refers to a technique used in communicating secretly using the legal traffic as the channel through which secret information is transferred over a network that is not trusted [20]. For the first time in 2003, the concept was introduced by Szczypiorski [21]. The techniques used in network steganography to facilitate hidden communication are those that make use of network protocols or correlations between them as a channel [22]. It is noteworthy that an observer (a third party) who is not aware that the steganography method is in use is also unaware of the exchange of concealed data through the carrier channels. There are three major kinds of network carrier channels:

- Covert storage channel: in this channel, the secret information is embedded into areas where the network protocols are redundant. One of the merits of using this method is the fact that it is easily implemented, while on the other side, its demerit is that it can easily be detected by extant methods [23-25].
- Covert timing channel: here, delivery of concealed information is achieved through the exploitation of time-relevant events of network packets and delivers the secret information by exploiting time-relevant events of network packets and it offers more secrecy than the covert storage type. In general, this category can be categorized into four major subclasses including: OnOff covert channel [26], interpacket delay- (IPD) based covert channel [27-30], packet sorting [31, 32], and combination-based ones [33].
- Hybrid Covert Channels: this type is one in which covert communication is carried out through the use of both time and storage channels combined together [34].

There are four main features that characterize network steganography communication: bandwidth, robustness, undetectability, and cost. The first three features, introduced by Fridrich in 1998 [35], are interdependent on each other and are normally represented as the three points of a triangle so as to illustrate these interdependences. For instance, a high level of robustness and undetectability is difficult to achieve when more bandwidth is required for secret communication. With this interdependence among the three features, there is a need for a trade-off between

them, in the event that a novel steganography system is introduced. The fourth feature, which is cost, shows the degradation of the carrier as a result of the procedure through which the secret data is inserted [36]. More so, it should be noted that the cost varies across the different channels, and can be detected through varying ways, such as the increase in bit error, increase in delay of packets, etc. It is noteworthy that among the four features of network steganography communication, undetectability is the most preferable.

2.3 The local area network (LAN)

A LAN refers to the different computers and computer peripherals (such as printers, disc storage devices, etc.) that are connected by high-speed data lines in a building or adjacent buildings [37]. With this network, high-bandwidth communication is provided over inexpensive transmission media. Originally, the aim of designing LANs was to enable the interconnection of a wide range of electronic infrastructure in an organization, so that local processing can be allowed, while also giving access to other devices connected to the network through a wired or wireless media [38]. For this LAN to be connected to the internet, a router is required, and it must be connected to a telephone line so that the transmission of data over longer distances can be achieved as shown in Figure 1.

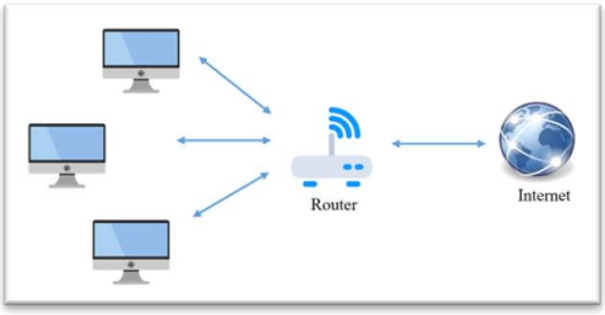

Figure 1: LAN Connected to the Internet through a Router.

2.4 The Internet Protocol version 4 (IPv4)

Since the introduction of IP, other versions have been produced, including IPv4, which is the fourth version that was introduced in the year 1978 and ascertained in the year 1981. The application of this protocol is seen in both the Internet layer of the TCP/IP model as well as in the network layer of the OSI Model. Therefore, most traffic of the routes is the responsibility of this protocol [39]. The length of the IPV4 header is 20 to 60 bytes in length and is made up of information that is critical to routing and delivery, and it is also made up of 13 fields, as seen in figure 2 [40].

- Version field: This field is a 4-bit version indicator. The value of the IPv4's four bits is set to 0100, which means four in binary.
- Internet Header Length (IHL): this field is of 4 bits in size. With this element of the header, the number of 32-bit words that exist in the header. The IPv4 headers vary in size, ranging between 20 bytes and 60 bytes, and as such, it is employed in specifying the header's size so that errors can be avoided.

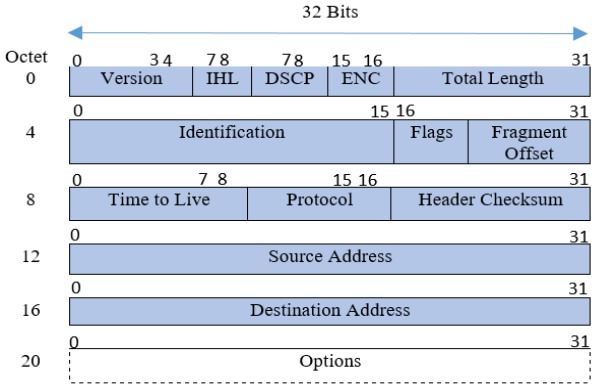

Figure 2: IPv4 Header Format Component.

- Type of Service: ToS, which is known as Differentiated Services Code Point (DSCP), is a field that is used in providing characteristics that are associated with quality of service like for Voice over IP (VoIP) calls or data streaming.
- Explicit Congestion Notification (ECN): through the use of ECN, notifications about network congestions are sent to the receiver or sender. This feature is less essential, and it is not supported by one end, the other endpoint does not use it as well.
- Total Length: The length of this field is 16 bit and the length of the whole datagram can be ascertained using it. An IP datagram's size ranges from 20 bytes to 65,535 bytes. In practice, it is expected that all hosts should have the ability to read 576-byte datagrams. In an event that the size of a datagram is too large for the hosts within the network, then the use of fragmentation is the employed host.
- Identification (ID): The role played by the ID field is essential as it helps with the identification of the unique segments of an IP's datagram. It has been suggested by some experts that the use of this field can be employed other areas such as the addition of information for packet tracing, etc.
- Flags: The flag is a 3 bits field that is employed in controlling and identifying segments. Their tentative configuration can be as follows:
  - ✓ Bit 0: this is reserved and has to be set to zero.
  - ✓ Bit 1: DF denoting do not fragment.
  - ✓ Bit 2: MF representing more fragments.
- Fragment Offset: The length of this field is 13 bits, it is used to assign the fragment offset relative to the start of the IP datagram, which when it was not fragmented. It is expected that a fragment's first offset be fixed at 0. The maximum possible offset is 65528.
- Time to live: which is also abbreviated as TTL is an 8-bit that is representative of the maximum time that the datagram can exist within the internet system. The measurement for this time is done in seconds, and in an event that the value of TTL is zero, the datagram is eliminated.
- Protocol: This field is used to show which protocol is utilized in the data part of the datagram. For instance,

the number 6 represents TCP, while the UDP protocol is denoted using the number 17.

- The header's checksum: is a field with a length of 16 bits, and it is employed in checking for errors in the header. At every hop, a comparison is carried out between the header and its checksum value, and if there is no correspondence between the two, the packet is discarded. It is important to note that this is only applicable to the header, and the data field is handled by the protocol of the header.
- Source Address: This is a 32-bit source address for an IPv4 packet.
- Destination Address: This is a 32 destination address, and it also carries the address of the receiver.
- Options: This is an optional field of the IPv4 header, which is only employed in the event that the set value of IHL is greater than 5. Contained in these options are the settings and values for everything associated with security, timestamp, loose source routing, record route, and strict source routing, as illustrated in Figure 3 below.

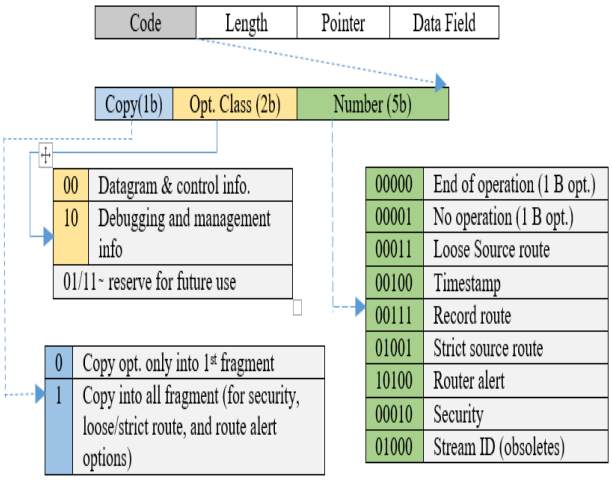

Figure 3: IPv4 Options.

2.5 IP Timestamp Option's Structure

The IP timestamp option's structure is depicted in Figure 4 [13]. Option type has a value of 68 decimal (i.e., copy flag = 0, option class = 2 and option number = 4); option length = the number of octets with a maximum of 40 (limited by IHL = 15); offset = the number of octets from the beginning of space for next timestamp option. It is set to one, an odd number, when the header no longer has space to accommodate timestamps; overflow = the number of IP modules that cannot register timestamps due to lack of space; the flag has 3 valid interpretations: =

- ✓ 0 – denotes time stamps only.
- ✓ 1 -- each timestamp is preceded with the internet ID of the registering entity.
- ✓ 3-- Internet ID fields are predetermined. The timestamp of an IP module is only registered by the module itself if there is correspondence between its own ID and the subsequent specified internet ID.

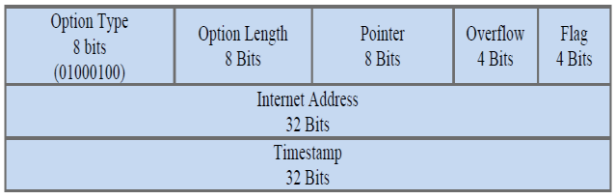

Figure 4: IP timestamp option's structure.

3 Related Work

The Network Steganography field is a new area of research that has emerged in recent times, but the research work carried out in this emerging area is limited, especially in terms of its implementation in in IPv4. Experts have suggested the use of several popular protocols for the implementation of steganography in IPv4. In this section, previous works are presented with a special focus on network steganography. In the work done by Bedi and Dua [13], the authors recommended that the Overflow field of the Timestamp option of IPV4 be used over a LAN. Normally, this is utilized for network monitoring and measurement. In another work, done in [41], Muhajjar and Badr proposed the creation of a covert channel using the Flow Label Field. In their system, the use of Pseudo-random number generators (PRNG) is employed in generating the keys for encryption/decryption. The authors also proposed the application of RC6 in CBC mode so as to enable the encryption/decryption of secret data, subsequent to the acquisition of the ciphertext, and the MAC is calculated using the authentication code, and then the values are concealed within the IPv6 flow label field. More so, in the work done by Bedi and Dua in [42], the authors proposed that extension headers be used for convert communication over IPV6. With their proposed method, 5 bits of covert data per IPV6 packet can be converted. In another work, Bedi and Dua [43] presented an algorithm ARPNetSteg which performs the implementation of Network Steganography through the use of Address resolution protocol. The robustness of the proposed method is such that, maximum of 44 bits of covert data per ARP reply packet can be transferred. The use of six storage and two timing covert channels in the Constrained Application Protocol (CoAP) was proposed by Mileva et al. in [44]. The covert channels proposed in their study can be suitably used in sending messages that are not lengthy. More so, in this method, the total number of hidden data bits transmitted per CoAP message or its Packet Raw Bit Rate (PRBP) for each covert channel is prescribed.

4 Proposed System

The proposed network steganography system is designed which involves the use of an IPV4 is employed as cover media that operates over a Local Area Network. The aim of the proposed system is to improve the security of secret information by combining two methods of security, including steganography and cryptography. These two are combined so that their unique benefits can be jointly leveraged upon, Given that both techniques play different

Table 1: Summary of the Related Works.

No.	Year	Title	Point focused
1	2020	Network steganography using the overflow field of timestamp option in an IPv4 packet	• Use of Overflow field Timestamp option in an IPv4 packet for data hiding. • 20 bits/s data rate achieved. • Difficult to detect the possibility of covert communication.
2	2018	Secure Data Communications using Cryptography and IPv6 Steganography	• Data encrypted using CBC-RC6 algorithm before embedding • Hidden in the flow label field of IPHeader
3	2020	Network Steganography Using Extension Headers in IPv6	• Given method for hiding secret data based on network steganography technique in the TCP/IP packet headers. • Less efficient in terms of capacity.
4	2020	ARPNetSteg: Network Steganography using Address Resolution Protocol	• Use the ARPNetSteg algorithm that implements Network Steganography using the Address resolution protocol. • 44 bits per ARP reply packet capacity achieved.
5	2018	New covert channels in Internet of Things	• The use of six storage and two-timing covert channels in the Constrained Application Protocol (CoAP)

roles (steganography is used in concealing the existence of the message, whereas, cryptography causes distortion to the message). The keys used in the processes of encryption and decryption were generated through the application of a cryptographically secure pseudo-random number generator (CSPRNG) was made. Upon the generation of the encryption/decryption key, the implementation of the CBC-RC6 encryption is done. After the ciphertext has been obtained, it is then embedded within the overflow field of the timestamp option of an IPV4 header. The basic architecture of the proposed system is illustrated in Figure 5.

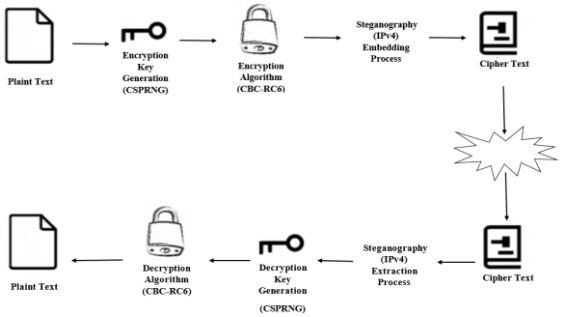

Figure 5: Basic architecture of proposed network steganography system.

4.1 Cryptographically Secure Pseudo-Random Number Generator (CSPRNG)

PRNGs are based on mathematical functions stemming from an initial condition to generate deterministic sequences over a long period. Such PRNGs are characterized by excellent mathematical properties like reproducibility, repeatability, and fast execution. Despite the fact that there are different kinds of PRNGs, the cryptographically secure PRNG remains the most suitable for cryptography. A CSPRNG is characterized by unpredictability and computational infeasibility for the generation of the initial bits of data. In cryptographic methods, the use of CSPRNGs is employed in providing cryptographic services such as hashing algorithm, encryption, digital signature, and generation of keys. The algorithm contains the pseudocode of the proposed technique as shown in figure 6.

Algorithm 1: Generation of CSPRNG.

Pseudocode: Generation of Optimized Pseudo-random binary Sequence
Output: Pseudo-random binary sequence
Procedure:
initial seed value of $x_0 \in (0,1)$ and $\gamma \in [4,31]$.

$$\eta_1 \leftarrow \left\lfloor \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{\lfloor \frac{1}{2} \rfloor}{\gamma}} \right\rfloor$$
$$\eta_2 \leftarrow \left\lfloor \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{\lfloor \frac{1}{2} \rfloor}{\gamma}} \right\rfloor$$

for $i = 1 : N$ **do**
if $\gamma \leq 4$

$$x_{i+1} \leftarrow [\gamma x_i (1 - x_i)]$$

else
if $x_i \geq \eta_1$ and $x_i \leq \eta_2$

$$x_{i+1} \leftarrow \frac{\gamma x(1-x)(mod\ 1)}{\frac{1}{2}\ (mod\ 1)}$$

else

$$x_{i+1} \leftarrow \gamma x(1-x)(mod\ 1)$$

end if
end if
if $x_i \geq 0.1$ and $x_i \leq 0.6$

$$y_j \leftarrow x_i$$
$$y_j \leftarrow y_i \times 10^{10}\ mod\ 1$$

if $y_j \geq \tau$

$$y_j = 1$$

else

$$y_j = 0$$

end if

$$j \leftarrow j + 1$$

else
discard x_i
end if
end for
y_j is the resultant binary sequence

Figure 6: The pseudo code of algorithm 1.

4.2 Encryption

Encryption is a process that involves the use of RC6 encryption algorithm in CBC mode, which is commonly used, because of its ability to counter the major limitations of the EBC mode by XORing bits of the input plaintext block with the previously ciphered block prior to the

process of encryption. Afterward, every ciphertext block will depend on all the blocks of the plaintext up to the current point. During the process of decryption, this effect is eliminated by the process of Xoring [1]. The initialization of the process of enciphering (RC6) is initiated by a dummy selected message (block of a defined length that is regarded as the Initialization Vector (IV)). Each encryption process requires a new and special IV value alongside the same key. The purpose of the IV is to ensure the acquisition of different ciphered blocks in an event that the encryption of the same original plaintext block is done several times individually through the use of the same secret key. Thus, each ciphertext is reliant on the IV value and the whole plaintext blocks preceding that block. Simply put, the CBC function mode involves the use of a serial dependence method [45]. Figure 7 shows the process of encryption involving the use of CBC-RC6.

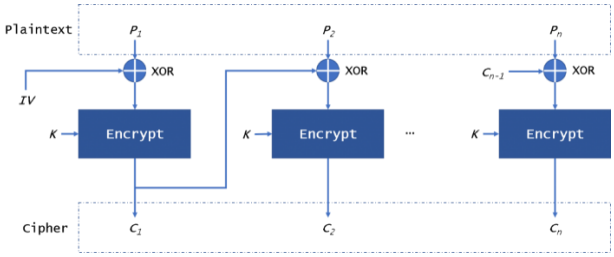

Figure 7: CBC-RC6 Encryption Process.

4.3 IPv4 Steganography

In the proposed system, the communication between every device and the internet occurs through the Transmission Control Protocol (TCP). The primary concept behind this work is to conceal secret data within the Overflow field of the Timestamp option of an IPv4 header without making the traffic packets suspicious. This means that the changes made to packet headers cannot be noticed by the host.

4.3.1 Embedding Process

The process of embedding is initiated at the side of the sender, who encrypts the plaintext. After the plaintext has been encrypting, the ciphertext is hidden within the overflow field of the timestamp option. The user's 20 bits of ciphertext is captured by the host and divided into five groups (each group has four bits), after which an IPv4 is crafted through the addition of five timestamp options, with each containing four bits within the overflow field. Typically, this field is used in carrying the several routers that were incapable to add the timestamp value. Here, the receiver's local IP address is already known to the sender, who uses it to deliver the IP packet to the receiver over TCP.

4.3.2 Extraction Process

In order to extract the concealed data, the receiver executes a python program, with all the received packets sniffed, while the TCP segment sent by the sender with a destination port of 54340 is captured. All the timestamp options are read by the python program starting from the captured packets, and afterward, the four bits of data are extracted from the Overflow field of each option. Then the encrypted sender's 20-bit message is read by combining the extracted bits. Subsequently, the decryption key is generated by the receiver through the use of the CSPRNG proposed in this study, and then CBC-RC6 decryption.

4.4 Decryption

Here, the plaintext is extracted by the receiver using the RC6 decryption algorithm in CBC mode. The steps of CBC-RC6 decryption are shown in detail in figure 8.

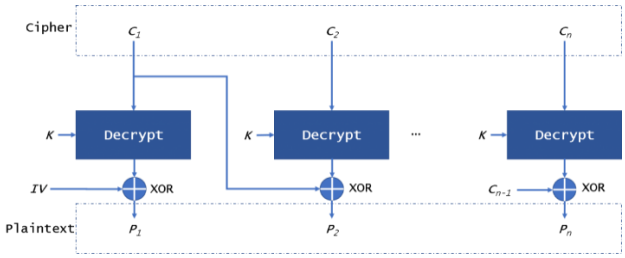

Figure 8: CBC-RC6 Decryption Process.

5 Simulation Environment

The use of EVE-NG was employed in the simulation of the processed system as illustrated in Figure 9. The topology for the simulation consists of the following devices:

- Router: A Cisco 2900 router was used in the proposed system to ensure that the business needs of customers are met, while the efficiency, capacity, and bandwidth are increased based on the growth of the network.
- Switch: The Cisco Catalyst 3560 seemed to be the most appropriate access layer for the proposed system; this switch helps in ensuring that the highest level of productivity is achieved.
- Host A: The host (A) refers to the entity which sending the secret message with the aim of communicating with a receiver in a confidential manner. Packets containing the secret information are crafted and sent through the scapy python's library. Scapy is a powerful Python-based interactive packet manipulation program and library that has the ability to forge or decode packets containing many protocols. This program is also able to send the forged packets, capture store them through the use of pcap files. It also carries out the matching of requests and responses.
- Host B: The host (B) refers to a receiver of secret message that awaits the arrival of the secret data from the host (A) over the Local Area Network. In this work, the TCP protocol is employed at the Transport Layer. The reason for selecting this protocol is that it performance data transfer task between two computers that are linked over the network with a high level of reliability. More so, it has been used previously in network applications where reliable and secure connection is needed because it ensures that data packets are intact and not lost during the process of transmission. Thus, in this work, the TCP server is programmed and executed in the proposed system to

ensure that the incoming segment is received at port 54340. After a TCP segment is received by this entity at port 49152, the IP packet header in the segment is then scanned.

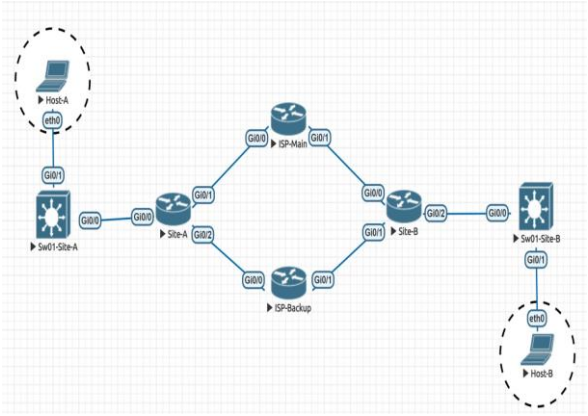

Figure 9: Diagram of the EVE-NG Topology

6 Results and Discussion

The first step in this work involved the use of a highly sensitive cryptographic algorithm that demonstrates high sensitivity to even minor changes in the key. In this study, random keys of length 128-bits are generated with the change of one bit at least significant bit (LSB) positions, as given in Table 1. The generation of CSPRNGs is achieved by mapped $x0$ and random chosen fixed control parameter $\gamma = 31$. The experimental results shown in Table 1 revealed that the CSPRNGs are not related and they demonstrate a high level of sensitivity to change in key.

Table 2: Results of the CSPRNGs.

Keys	Secret Key
1	ABCDEA01234567899876543210AFECDB
2	ABCDEA01234567899876543210AFECDC
3	ABCDEA01234567899876543210AFECDD
4	ABCDEA01234567899876543210AFECDE
5	ABCDEA01234567899876543210AFECDF
6	ABCDEA01234567899876543210AFECDG

The practical aspect of the proposed technique is evidenced in the fact that once the message is decrypted by the intruder, the receiver will receive a large number of packets that result in heavy bulks of data. This step involved the analysis of the RC6 algorithm so as to facilitate the evaluation of the complexity of the time needed for alphabets, numbers, alphanumeric, as well as for a different number of inputs (10, 20, 30, and 40) characters. The results of the analysis for every type of input based on time (measured in milliseconds) is presented in Figure 10. It is noteworthy that in this step, just like the process of encryption, the time required for processing is measured in milliseconds, and everything is done within a short period of time, not requiring much time, where information is sent, received, and decoded by the receiver in milliseconds.

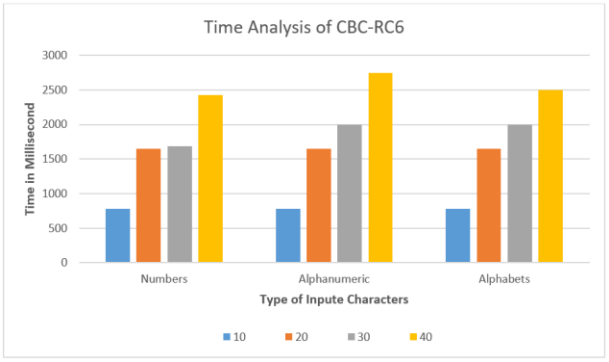

Figure :10 Representation of the Analysis of RC6.

To embedding secret data, 20 bits of hidden data per packet are transferred from sender to receiver which can be seen from the Wireshark captures, as illustrated in Figure 11. The hidden data is received as input from the sender, encased in the Timestamp option of the IPv4 packet, and transmitted to the receiver. Following that, the receiver analyzes the IPv4 packet's Timestamp option to extract the hidden data from the Overflow fields of five timestamp options.

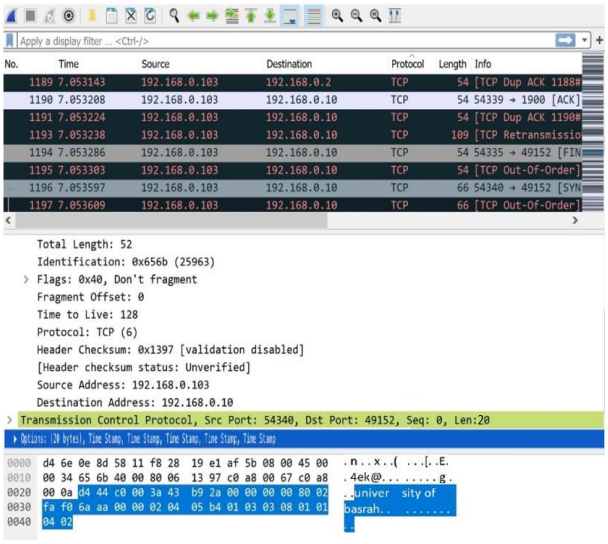

Figure 11: Packets Sent From sender (Host A) to receiver (Host B) Captured by Wireshark.

When comparing the results of the proposed method with the previous works reviewed in table 1, we conclude that the proposed method offers a higher security level than that of other extant techniques, because other authors only employed the use of steganography methods, while the proposed system is a combination of both cryptography and steganography techniques.

7 Conclusion and Future Works

In this work, a method has been proposed to enable the security of channels of communication between communicating parties. The proposed system is a combination of cryptography and network steganography in IPv4, and they were implemented for secret communications with the use of functions contained in a

single IPV4 packet header. Also, in this work, five timestamp options were created in one IPv4 packet header. The results of the experiments carried out in this work showed that this channel has the ability to convey 20 bits of data per packet. The proposed technique was basically developed and implemented on a LAN setup, and it makes use of TCP at the transport layer. The high level of reliability of the TCP is the basis for its use in this work. For cryptography, the implementation of the RC6 algorithm was carried out in CBC mode to ensure that a higher level of security is achieved. The contribution made by the proposed technique is that it offers a higher security level than that of other extant techniques, because other authors only employed the use of steganography methods, while the proposed system is a combination of both cryptography and steganography techniques. More so, in comparison to other previous works, the process of embedding is characterized by more complexities than that of previously proposed systems. With the proposed system, it is difficult for an intruder to hijack the system, because even if the intruder is able to capture the packets, they need to have knowledge of the key, the encryption algorithm that was utilized, and the manner in which the information was embedded in the overflow field; within this period of events, the receiver must have received many packets that will result in the detection of the malicious activities of the intruder. Future works should be focused on the identification and exploration of alternative covert channels, as well as their application over the internet.

References

[1] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, et al., "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," IEEE Access, vol. 8, pp. 103200-103218, 2020.

[2] H. Al-Hashimy, A. Hamoud, and F. Hussain, "The Effect of Not Using Internet of Things in Critical life Situations in the Health Field and the Effect on Iraqi Profitability: Empirical Study in Basra," Journal of Southwest Jiaotong University, vol. 54, 2019.

[3] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," Optics and Lasers in Engineering, vol. 124, p. 105816, 2020.

[4] W. A. Awadh, A. S. Hashim, and A. Hamoud, "A Review of Various Steganography Techniques in Cloud Computing," University of Thi-Qar Journal of Science, vol. 7, pp. 113-119, 2019.

[5] M. I. S. Reddy and A. S. Kumar, "Secured data transmission using wavelet based steganography and cryptography by using AES algorithm," Procedia Computer Science, vol. 85, pp. 62-69, 2016.

[6] W. A. Awadh and A. S. Hashim, "Using steganography for secure data storage in cloud computing," 2017.

[7] A. S. Saber and W. A. Awadh, "Steganography in MS Excel Document Using Unicode System Characteristics," J. Basrah Res. Sci, vol. 39, pp. 0-19, 2013.

[8] R. K. Yadav and M. Kushwaha, "Message Hiding Using Steganography and Cryptography," 2018.

[9] G. D. Moody, M. Siponen, and S. Pahnila, "Toward a unified model of information security policy compliance," MIS quarterly, vol. 42, 2018.

[10] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," ACM Computing Surveys (CSUR), vol. 51, pp. 1-35, 2018.

[11] M. Hashim, M. S. MOHD RAHIM, and A. A. ALWAN, "A REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN," Journal of Theoretical & Applied Information Technology, vol. 96, 2018.

[12] M. S. Taha, M. S. M. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of steganography and cryptography: A short survey," in IOP conference series: materials science and engineering, 2019, p. 052003.

[13] P. Bedi and A. Dua, "Network steganography using the overflow field of timestamp option in an IPv4 packet," Procedia Computer Science, vol. 171, pp. 1810-1818, 2020.

[14] N. Kheshaifaty and A. Gutub, "Preventing multiple accessing attacks via efficient integration of captcha crypto hash functions," Int. J. Comput. Sci. Netw. Secur.(IJCSNS), vol. 20, pp. 16-28, 2020.

[15] A. Gutub and F. Al-Shaarani, "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons," Arabian Journal for Science and Engineering, vol. 45, pp. 2631-2644, 2020.

[16] M. G. Alkhudaydi and A. A. Gutub, "Integrating light-weight cryptography with diacritics Arabic text steganography improved for practical security applications," Journal of Information Security and Cybercrimes Research, vol. 3, pp. 13-30, 2020.

[17] A. S. S. AL-Mozani and W. A. J. Awadh, "A new text steganography method by using non-printing unicode characters and unicode system characteristics in English/Arabic documents," JOURNAL OF THI-QAR SCIENCE, vol. 3, 2012.

[18] A. E. Ali, "A new text steganography method by using non-printing unicode characters," Eng. & Tech. Journal, vol. 28, 2010.

[19] B. Seok, J. C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan, and J. H. Park, "Secure D2D communication for 5G IoT network based on lightweight cryptography," Applied Sciences, vol. 10, p. 217, 2020.

[20] M. Wang, W. Gu, and C. Ma, "A Multimode Network Steganography for Covert Wireless Communication Based on BitTorrent," Security and Communication Networks, vol. 2020, 2020.

[21] K. Szczypiorski, "Steganography in TCP/IP networks," in State of the Art and a Proposal of a New System–HICCUPS, Institute of

Telecommunications' seminar, Warsaw University of Technology, Poland, 2003.
[22] B. Jankowski, W. Mazurczyk, and K. Szczypiorski, "PadSteg: Introducing inter-protocol steganography," Telecommunication Systems, vol. 52, pp. 1101-1111, 2013.
[23] M. A. Elsadig and Y. A. Fadlalla, "Survey on covert storage channel in computer network protocols: detection and mitigation techniques," International Journal of Advances in Computer Networks and Its Security, vol. 6, pp. 11-17, 2016.
[24] R. Sun, L. Shi, C. Yin, and J. Wang, "An improved method in deep packet inspection based on regular expression," The Journal of Supercomputing, vol. 75, pp. 3317-3333, 2019.
[25] Y. Jiang, M. Zhao, C. Hu, L. He, H. Bai, and J. Wang, "A parallel FP-growth algorithm on World Ocean Atlas data with multi-core CPU," The journal of Supercomputing, vol. 75, pp. 732-745, 2019.
[26] S. Cabuk, C. E. Brodley, and C. Shields, "IP covert timing channels: design and detection," in Proceedings of the 11th ACM conference on Computer and communications security, 2004, pp. 178-187.
[27] X. Zi, L. Yao, L. Pan, and J. Li, "Implementing a passive network covert timing channel," Computers & Security, vol. 29, pp. 686-696, 2010.
[28] T. Zhu, Y. Lin, Y. Liu, W. Zhang, and J. Zhang, "Minority oversampling for imbalanced ordinal regression," Knowledge-Based Systems, vol. 166, pp. 140-155, 2019.
[29] S. Gianvecchio, H. Wang, D. Wijesekera, and S. Jajodia, "Model-based covert timing channels: Automated modeling and evasion," in International Workshop on Recent Advances in Intrusion Detection, 2008, pp. 211-230.
[30] G. Liu, J. Zhai, and Y. Dai, "Network covert timing channel with distribution matching," Telecommunication Systems, vol. 49, pp. 199-205, 2012.
[31] X. Zhang, C. Liang, Q. Zhang, Y. Li, J. Zheng, and Y.-a. Tan, "Building covert timing channels by packet rearrangement over mobile networks," Information Sciences, vol. 445, pp. 66-78, 2018.
[32] X. Zhang, L. Zhu, X. Wang, C. Zhang, H. Zhu, and Y.-a. Tan, "A packet-reordering covert channel over VoLTE voice and video traffics," Journal of Network and Computer Applications, vol. 126, pp. 29-38, 2019.
[33] Z. Pan, X. Yi, Y. Zhang, B. Jeon, and S. Kwong, "Efficient in-loop filtering based on enhanced deep convolutional neural networks for HEVC," IEEE Transactions on Image Processing, vol. 29, pp. 5352-5366, 2020.
[34] A. Salih, X. Ma, and E. Peytchev, "Implementation of hybrid artificial intelligence technique to detect covert channels attack in new generation internet protocol IPv6," in Leadership, Innovation and Entrepreneurship as Driving Forces of the Global Economy, ed: Springer, 2017, pp. 173-190.
[35] J. Fridrich, "Applications of data hiding in digital images," in ISSPA'99. Proceedings of the Fifth International Symposium on Signal Processing and its Applications (IEEE Cat. No. 99EX359), 1999, p. 9 vol. 1.
[36] W. Mazurczyk, S. Wendzel, I. Azagra Villares, and K. Szczypiorski, "On importance of steganographic cost for network steganography," Security and Communication Networks, vol. 9, pp. 781-790, 2016.
[37] O. Goni, "IMPLEMENTATION OF LOCAL AREA NETWORK (LAN) AND BUILD A SECURE LAN SYSTEM FOR ATOMIC ENERGY RESEARCH ESTABLISHMENT (AERE)," Int. J. of Electronics Engineering and Applications, vol. 9, 2021.
[38] N. S. Tarkaa, P. I. Iannah, and I. T. Iber, "Design and simulation of local area network using cisco packet tracer," The International Journal of Engineering and Science, vol. 6, pp. 63-77, 2017.
[39] Z. Hamid, S. Daud, I. S. A. Razak, and N. A. Razak, "A Comparative Study between IPv4 and IPv6," ANP Journal of Social Science and Humanities, vol. 2, pp. 68-72, 2021.
[40] A. M. Bahaa-Eldin, "Tutorial II: Network Security," in 2020 15th International Conference on Computer Engineering and Systems (ICCES), 2020, pp. i-ii.
[41] A. M. Ra'ad and F. A. Badr, "Secure Data Communications using Cryptography and IPv6 Steganography," International Journal of Engineering & Technology, vol. 8, pp. 163-168, 2019.
[42] P. Bedi and A. Dua, "Network Steganography Using Extension Headers in IPv6," Singapore, 2020, pp. 98-110.
[43] B. A. Punam, Dua, "ARPNetSteg: Network Steganography using Address Resolution Protocol," International Journal of Electronics and Telecommunications, vol. 66, 2020.
[44] A. Mileva, Aleksandar, VelinovDone, Stojanov, "New covert channels in Internet of Things.," p. 7, 2018.
[45] R. Donev, A. Alsadoon, P. W. C. Prasad, A. Dawoud, S. Haddad, and A. Alrubaie, "A novel secure solution of using mixed reality in data transmission for bowel and jaw surgical telepresence: enhanced rivest cipher RC6 block cipher," Multimedia Tools and Applications, vol. 80, pp. 5021-5046, 2021/02/01 2021.