Journal of Computer Science & Computational Mathematics, Volume 8, Issue 4, December 2018
DOI: 10.20967/jcscm.2018.04.001

Packet Length Covert Channels Crashed

Muawia A. Elsadig[1,2*], Yahia A. Fadlalla[2,3]

[1]Imam Abdurrahman Bin Faisal University, P.O. Box 1982, Dammam, Saudi Arabia
[2]College of Computer Science and Technology, SUST, Khartoum, Sudan
[3]Lead Consultant/Researcher, InfoSec Consulting, Hamilton, Ontario, Canada
[*]Corresponding author email: muawiasadig66@gmail.com

***Abstract*:** Advanced developments in network security tools and techniques have inspired attackers to find alternative ways to bypass them. A network covert channel is a wide-open door for attackers to leak confidential information or to convey malicious activities without being detected. Moreover, the rapid development in network technology and its applications provides a rich platform for developing different covert channel scenarios. A packet length covert channel is a network illicit communication channel that is featured as one of the most difficult covert channels to detect. It generates a covert traffic that is typically similar to normal traffic; this renders such a channel to be virtually impossible to discover. This paper investigates one type of packet length covert channels which exploits the variation of the network packets' lengths to convey secret messages - this type of covert channels does not need any rules to be distributed prior to the initiation of a covert session as other packet length covert channels need. The paper contributes by presenting an elimination approach to resolve this type of covert channel. This approach is sufficiently capable to completely distort the communication session between any sender and receiver who wish to establish such a covert channel. The proposed approach is successfully tested and validated.

***Keywords*:** covert channel, security, detection, prevention, elimination, packet length covert channel, packet size covert channel, network protocols.

1. Introduction

A covert channel scenario was initially introduced in a single machine computing environment in 1973 by Lampson [1]. It was constructed in a multilevel security (MLS) environment, in which two processes are acting on behalf of two users with different security levels. These processes leak information from a high security level to a low security level in a manner that violates system security policies. In 1987, Girling extended the concept of a covert channel to network environments by introducing the first covert channel in local area network (LAN) [2]. This trend motivated the development of different scenarios and techniques to implement network-based covert channels. In result, many recent techniques have truly enriched the creation of undetectable network-based covert channels.

Covert channels are commonly categorized into two main types: storage and timing covert channels. In storage covert channel, one process can write into a storage location (i.e., a protocol field) and another process reads from that location. In timing channels, one process can signal secret information by modulating some aspect of system behavior over time while another process can observe and decode that information. On the other hand, some covert channels are constructed based on combining the two types together to form so called hybrid covert channels. This type of covert channel is posing serious threats, as it inherits the advantages of both types of covert channels, the high bandwidth feature of storage channels and the undetectable features of timing channels. Therefore, this hybrid style results in high bandwidth covert channels that are so hard to detect.

The packet length-based covert channel is an important type of network covert channel. It represents a new preference in this field due to its good performance in imitating the statistical features of real network packets [3]. Packet length-based covert channel exploits the length variations of network packets to modulate secret information. Covert users encode secret information using packet length variations, while the intended covert receiver observes and decodes back the secret message [4]. Each packet length or a group of packet lengths can be used to encode a piece of information and that is based on the method being used. Actually, many methods have been developed to leak conditional information based on network packet-length. Recently, this type of covet channel has received attention due to its undetectable features [5, 6].

To the best of our knowledge, to this end, no sufficient solution is presented to deal with such type of covert channel that is under our investigation in this paper. This motivates us to contribute to this area by presenting our proposed approach which is expected to fully eliminate any potential packet length-based covert channel that is envisioned to leak secret information covertly. This paper is an extended version of our work presented in [7].

This section gives a general overview of covert channels, while the rest of the paper is organized as follows: the next section sheds lights on covert channel development. Section 3 addresses the so-called prisoners' problem which is considered as a common model to demonstrate the typical covert channel scenario. It illustrates the basic concept of a covert channel. A thorough investigation of packet-length covert channel related work is presented in Section 4. This section also gives details on packet length covert channel development and the countermeasures. Our proposed approach is illustrated in Section 5 and subsequently Section 6 presents our approach implementation and results. Section 7 validates our findings and then the paper is concluded in Section 8, while the future work is presented in Section 9.

2. Covert Channel Development

A covert channel intends to leak a secret message to an unauthorized user in a way that it breaks up the system security policy by exploiting regular communication procedures. A covet channel can cause massive risk when exploited to pass malicious activities.

A recent literature review on covert channel countermeasures shows difficulties in countering such hidden threats. The common countermeasures are either applied to eliminate, reduce bandwidth, detect, or to document covert channels [4]. In addition, each solution to covert channels is used to target one type of covert channel instead of focusing on common behaviors of multiple covert channels, which lead to reduce overheads.

Some authors [5] have thoroughly reviewed network covert channel types, techniques, development, and countermeasures. They highlighted that more work in covert channel prevention and detection is still required as covert channel techniques are rapidly developed due to the rapid development in computer network protocols and network technologies. Moreover, deep knowledge in covert channel techniques is highly encouraged to assist in developing suitable countermeasures that sufficiently deal with this kind of threat.

Recently, Elsadig and Fadlalla summarized some factors that have the most impact on developing covert channels and magnifying their threats [6]. These factors involve:

- The advanced development in network technology, the Internet of Things (IoT) which represents a rich area of different scenarios of covert channels, cloud computing, data centers and virtualization techniques
- Switching techniques, in which a covert channel can switch itself from one protocol to another or from one field to another in a given protocol or from one network segment to another.
- Internal control protocols technique, which uses a micro protocol to provide reliable communication and dynamic routing to the covert message.

According to these findings, Elsadig and Fadlalla introduced a new concept of network covert channel. They call it a network covert channel triangle (DSM - Development, Switching, and Micro-protocol), which involves three elements that have the most direct impact on motivating, encouraging and developing covert channels.

All the above indicates the ongoing development of covert channels and the security risk that they can pose. Indeed, to this end, we can say that our confidential information is at risk and the security professionals are facing a real challenge.

Due to the undetectable features of covert channels, it is noteworthy to say that, some uses of covert channels to secure confidential information were presented. For example, network administrators exploit covert channels to distribute secret information among system clients. Furthermore, much work has been shaped to use covert channels legitimately. Interested readers are referred to more information regarding using covert channels for legal purposes [8-12]. However, this trend does not change the fact that covert channels present a dangerous threat. It is rapidly developed to leak secret information.

3. Typical Covert Channel Model

As it is illustrated in Figure 1, the typical concept of covert channels can be illustrated using a common model that is represented by the so-called prisoner's problem [13]. The prisoner's problem is considered as the standard of covert channel model that can be adapted to represent different scenarios of information hiding [14].

Imagine that Alice and Bob are arrested and put in a prison in which all communications between them are monitored. The possible channel for their communication is watched by so-called Wendy. If Wendy detects any suspicious communication, Alice and bob will be sent to separate prisons. Alice and Bob are aware of that and they don't want to lose their opportunity to plan for escape; therefore, they look for a way to establish a hidden communication channel to manage that. A channel that couldn't be seen by Wendy. This hidden channel is known as a covert channel. It passes secret information in a way that is unobservable by the monitoring system but somehow it exploits the regular communication channel itself. In terms of network, imagine that Alice and Bob are connected via networked computers that are monitored by a network administrator. So, when Alice and Bob succeed in establishing a hidden communication channel that couldn't be detected by the network monitoring system, a network covert channel exists. This scenario represents another type of covert channel, known as a network covert channel [15].

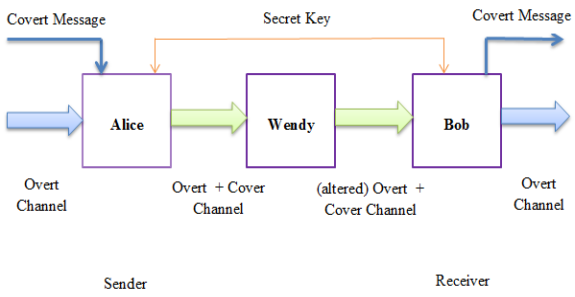

Figure 1. Typical Covert Channel Model [16]

4. Related Work

Since many protocols and applications generate random lengths of network packets (i.e. UDP protocol), hackers find this a good opportunity to develop a covert channel that is based on the packet length variation. They are exploiting these variations to encode secret information and then the intended receiver observes and decodes back the encoded information. In other words, each packet length can be used to encode a piece of a secret message. This type of covert channel is commonly known as a packet length-based covert channel. Initially, the packet length covert channel was developed by Padlipsky and rapidly spread and developed to pose real threats. The below subsections demonstrate the

historical background that reflects the fast growth of packet length covert channels.

Packet length covert channels were initially introduced by Padlipsky [17] and Girling [18], in which a secret message can be composed based on data link layer frame lengths. Both a receiver and a sender agree on shared rules to convey a secret message. A byte of covert message can be encoded by 256 different frame lengths [19]. However, these techniques introduce covert traffic that is easily detected through any detection mechanisms that rely on distinguishing between normal and abnormal traffic, since Padlipsky and Girling techniques cause notable changes in normal traffic.

A packet length covert channel proposed by Yao *et al.* was constructed based on a shared secret matrix, which includes selected unique lengths. This Matrix is somehow exchanged between covert users (a receiver and a sender). A sender uses the shared matrix to encode his covert message while the intended a receiver retrieves the encoded message using the same matrix [20]. The covert traffic of this technique fails to imitate normal traffic; therefore, the common detection methods are easily capable of detecting the presence of such a covert channel. In addition, Ji *et al.* practically proved that the above mentioned covert channels generate random distributed traffic, which is far more than the normal traffic. Therefore, these covert channels are vulnerable to detection methods [21]. This motivated Ji *et al.* to develop a packet length covert channel that has tamper resistance and is hard to detect. They claimed that their proposed channel delivers covert traffic that closely looks like normal traffic. They are basing their work on using normal packet lengths that are taken from real traffic as a reference to create covert traffic. However, Nair *et al.* practically implemented this covert channel and showed that the time series of the covert traffic package lengths are notably different from the time series of the normal lengths [22]. Therefore, their proposed detection method can easily detect the mentioned packet length covert channel. In addition, Ji *et al.* in a newer study [23] presented the shortcoming of their previous covert channel [21], and accordingly they proposed another packet length that has great resistance to network traffic detection methods. In 2011, Hussain introduced a packet length covert channel [24] that outperforms the above two mentioned covert channels in terms of covert channel capacity. Their covert channel has achieved high bandwidth for covert communication, and that is based on taking a slightly different way in utilizing both packet lengths and data payload to construct their covert channel. However, this covert channel is based on using the data payload as a carrier of a secret message and it is considered more complicated [25].

In 2013, Abdullaziz *et al.* took a different way by developing two packet length-based covert channels that did not depend on utilizing a shared secret key as previous techniques did [26]. Their covert channels introduce covert traffic that looks very closely like normal traffic, which increases the resistance against detection methods. Since a covert channel bandwidth of only one-bit size can easily allow the transmission of a system pin code which can lead to tremendous risk, Abdullaziz *et al.* do not pay attention to their covert channel bandwidth.

In 2014, Zhang *et al.* developed a packet length covert channel that closely imitates normal traffic [2] which complicates the way to detect such covert channel..

5. The Proposed Approach

This section introduces and describes our proposed approach, which is expected to resolve the packet length-based covert channel developed in one study by Abdullaziz *et al.* [26]. For demonstration, this section starts with an illustration of constructing a covert channel that will be used to evaluate our proposed approach since, to our knowledge, to this end, there is no available public dataset for this covert channel.

5.1 Constructing a covert channel

A covert channel is constructed based on the covert channel described by Abdullaziz *et al.* [26], which relies on changing the network packet lengths to modulate a secret (covert) message. Each packet length represents one bit of the secret message, in which an even value of a packet length represents '0' and an odd value represents '1'. Therefore, the modulating of a secret message is based on changing the network packet lengths according to the secret message itself. As an example, assume that a covert sender wants to send '100111101' as a secret message to a covert receiver over the following packets lengths (50, 70, 34, 67, 64, 19, 31, 65, and 89). In this scenario, the covert user should change the packets lengths according to the secret message. The first bit of the secret message is '1' so the packet length should be an odd value, therefore the sender changes the length '50' to '51' and keeps the second packet length '70' as it represents the second bit of the secret message which is '0' and so on. At the end, the modified traffic (covert traffic) will be as follows: (51, 70, 34, 67, 65, 19, 31, 66, and 89). The receiver can easily pick out the secret message.

Steps of constructing real covert traffic:

1. One can establish a Skype session between two Skype users, and then the Wireshark tool could be used to capture normal Skype traffic.
2. Using the Scapy tool, which is a library in Python language, the captured Skype traffic mentioned above can be modulated with a covert message to generate covert traffic.
3. Then, using Python language, this covert traffic can be injected into the network and it could be captured again to obtain real covert traffic.

These steps clearly demonstrate how covert traffic can be obtained practically, whereas the next section illustrates our proposed method to eliminate such types of covert channels.

5.2 Approach description

This section demonstrates the idea of our proposed method, which relies on increasing the length of one packet of each group of 8 packets lengths. As an example, imagine that we have covert traffic with 48 packets lengths, these 48 packets lengths contain 6 groups of 8 packets lengths. So, in this case, our proposed method changes only one packet length

from each group. The selection of a packet to be changed is done randomly.

Choosing to change only one packet length of each group of eight packets lengths is based on the assumption that this change leads to changing every character of a secret message, which ensures total change of the secret message. In result, this eliminates any covert communication that is based on exploiting the lengths of network packets to modulate a secret message. Each packet length can carry one bit of a secret message and it is given that, each byte of a secret message represents one character (i.e. “this is you” is a message of 11 characters including spaces). Therefore, changing one bit of a byte leads to changing the byte value and thus changing the character value. So, changing each character of a secret message will result in changing the whole message.

The below example demonstrates our approach concept. The illustration is given for only 8 packets lengths.

Example: assume that a covert user uses traffic with eight packets to modulate his/her secret message 'm' which is equivalent to ' 01101101' in bits. So accordingly, the packets lengths are being modified to form the covert traffic as illustrated in the first row of Table 1. After applying our proposed method, which relies on the changing of only one bit of each group of 8 packets lengths, the traffic will be as the one illustrated in the fourth row of Table 1. The covert receiver retrieves the covert message as 01001101 which is equivalent to “a” and thus the intended covert receiver received a totally different message. Imagine covert traffic with 800 packets lengths; the sender can use them to send a covert message with 100 characters. According to our message the receiver will get 100 totally different characters, which assures total change of the received message.

Table 1. The Approach Demonstration

Packets lengths with covert message	**34**	**15**	**71**	**80**	**67**	**37**	**18**	**77**
Covert message in bits	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**1**
Covert message in Char	**M**							
After Applying our approach, which is based on changing the length of only one packet length that selected randomly.	**34**	**15**	**72**	**80**	**67**	**37**	**18**	**77**
The covert message in bits	**0**	**1**	**0**	**0**	1	1	0	1
The covert message in char (is totally different than the sent one)	**A**							

Figure 2 shows the flowchart of our proposed approach, which clearly defines how it works. It randomly changes the length of one packet from each group of eight packets. While in the case that the number of packets is fewer than eight, it randomly selects any packet and changes its length (see Figure 2 which is clearly stated in this workflow.

6. Approach Implementation and Results

Randomly three groups of network packets (176 packets, 184 packets and 216 packets) from the captured packets are selected to encode the following secret messages respectively: “The pin code is ty54@h”, “The meeting will be at 7”, and “I will meet you on Thursday”. The number of packets is selected based on the length of a secret message. As an example, the first secret message required 176 packets lengths to be encoded, and the second secret message required 184 packets lengths to be encoded.

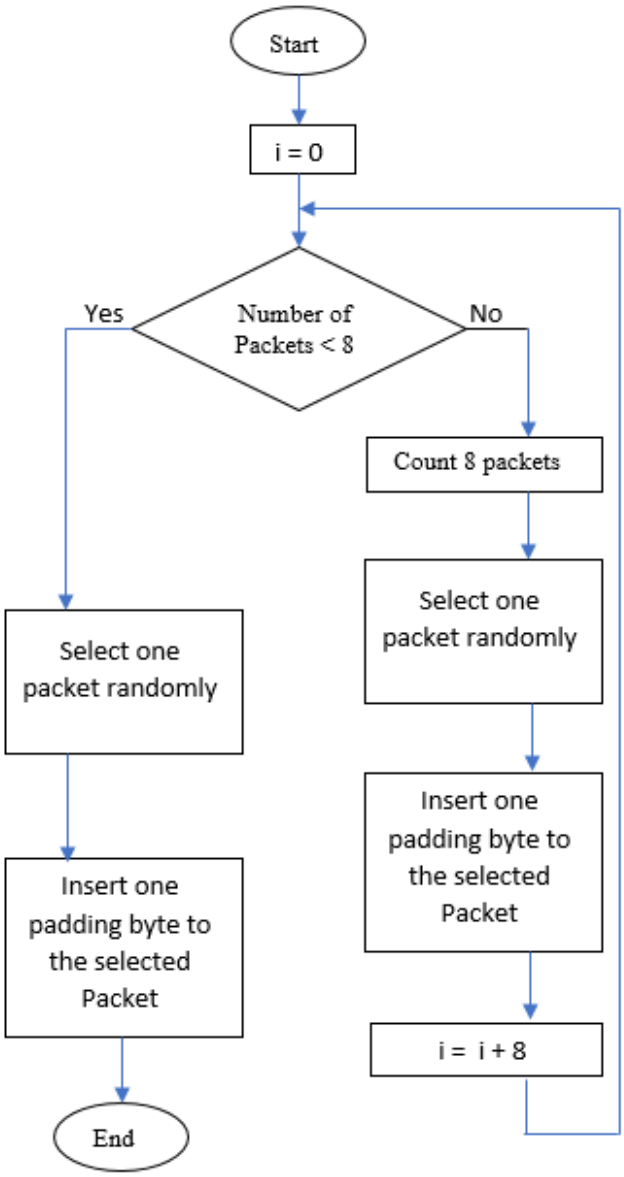

Figure 2. The Flow Chat of our Proposed Approach

Implementation steps:

1. 500 network packets (normal traffic) was captured using Wireshark.
2. Three groups of packets are selected from the captured packets as mentioned above (176,184,216).
3. The three secret messages (mentioned above) were encoded into the packets lengths of the selected groups using Scapy tool. The result of this step is three groups of covert traffic. Each one carrying one of the secret messages.
4. Then, our proposed approach is applied to each covert traffic separately. After applying our approach, and in all cases, the receiver decodes a message that is totally different from the secret message encoded by the sender.

Figures 3, 4 and 5 verify our findings in a graph style. Figure 3 shows a graph that represents the covert message, the message modulated by a covert sender who intends to send it to a covert receiver. The X axis represents the sequence of the covert message characters and the Y axis represents the decimal corresponding value of each character. Figure 4 shows the covert message after applying our proposed approach. It is clearly noticed that, the covet message is totally changed. Figure 5 shows both the original covert message and the modified covert message after applying our approach. The difference between them is clearly noticeable, which practically proves that our proposed approach can totally eliminate such types of covert channels by completely changing the covert message. So, the intended covert receiver receives a totally different message. This indicates that our proposed solution can fully eliminate any potential packet length covert channel with a successful rate of 100%. The next section is validated using two common text similarity measures.

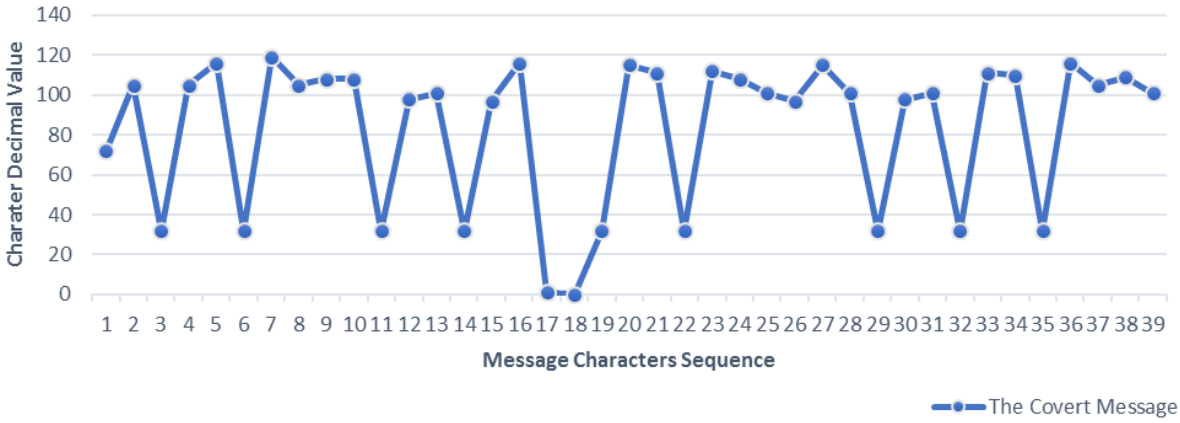

Figure 3. The Covert Message

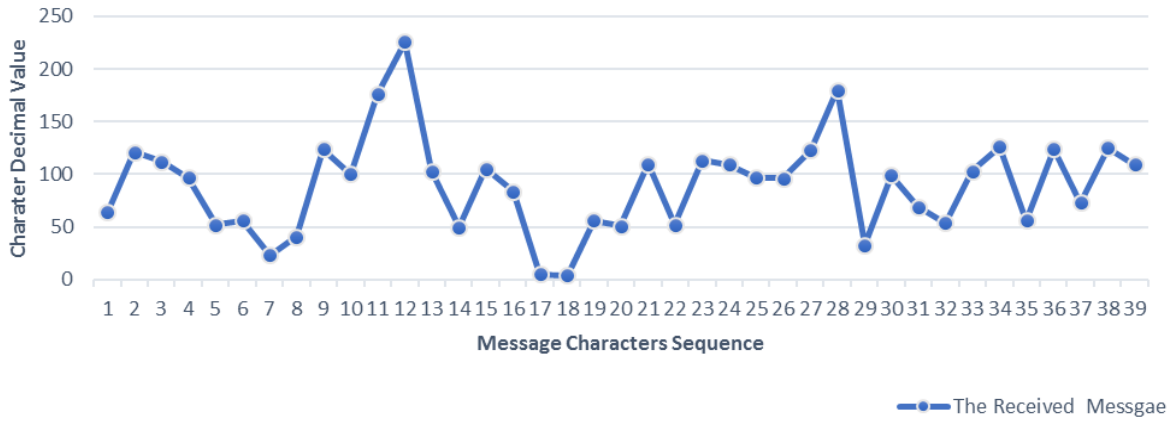

Figure 4. The Covert Message after Applying our Approach

7. Approach Validation

Our proposed approach was applied to 20 covert messages and accordingly 20 altered messages were obtained. Then, the two common text similarity measures (Cosine similarity and Dice coefficient) were used to check the similarity between the 20 covert messages and their altered messages that were obtained by applying our approach.

Cosine similarity is a popular method to compute the similarity of texts by treating them as vectors and calculating their cosine [27]. This delivers a value between 0 and 1; where 1 means the two texts are exactly the same and 0 indicates no similarity.

Mathematically, the cosine similarity between a text A and a text B is calculated as follows [28]:

$$Cosine\ Similarity = \vec{A}.\vec{B} / \| \vec{A} \| \| \vec{B} \|$$

Where,

$\vec{A}$ is a vector that is computed based on text A.

$\vec{B}$ is a vector that is computed based on text B.

$\|\vec{A}\|$ is the vector magnitude

Dice coefficient [29, 30] is a text similarity measure **(**term-based similarity measure) that is computed as follows:

*Dices coefficient = 2 *CT / (NA + NB)* [27].

Where,

CT: Common Terms in both string A and string B

NA: Number of terms in in string A

NB: Number of terms in in string B.

Table 2 shows the average measures of the aforementioned evaluation measures. Both cosine similarity and Dice coefficient indicate zero similarity which means no similarity between the original covert message and its altered form that is obtained by applying our proposed approach.

This indicates that a covert channel elimination rate of 100% is gained by applying our approach.

Table 2. Text Similarity Score

The similarity method	Cosine similarity	Dice coefficient
The average score	0.00	0.00

8. Conclusion

After a thorough investigation of packet length-based covert channel countermeasures and techniques, it is noteworthy to mention that up to this point, there is no solution presented to counter such type of packet length covert channels. In addition, any propose security solution should take into account the performance of network systems [31, 32]. In other words, any security solution has to attain a balance to keep a system performance intact [33]. In this paper, an efficient solution to resolving packet length-based covert channels –investigated in this paper - is presented. Our solution is based on changing the sent covert message that is being encoded using packet length variations, so the intended receiver can retrieve a completely different message from the message sent by the sender. This results in breaking up the communication channel between the covert sender and receiver and thus eliminates any potential covert channel that they intend to establish. Our approach has been practically verified as it gained a success rate of 100% – we verified that each time the receiver gets a message that is totally different from the covert message sent by the sender – therefore; the communication between them is fully distorted.

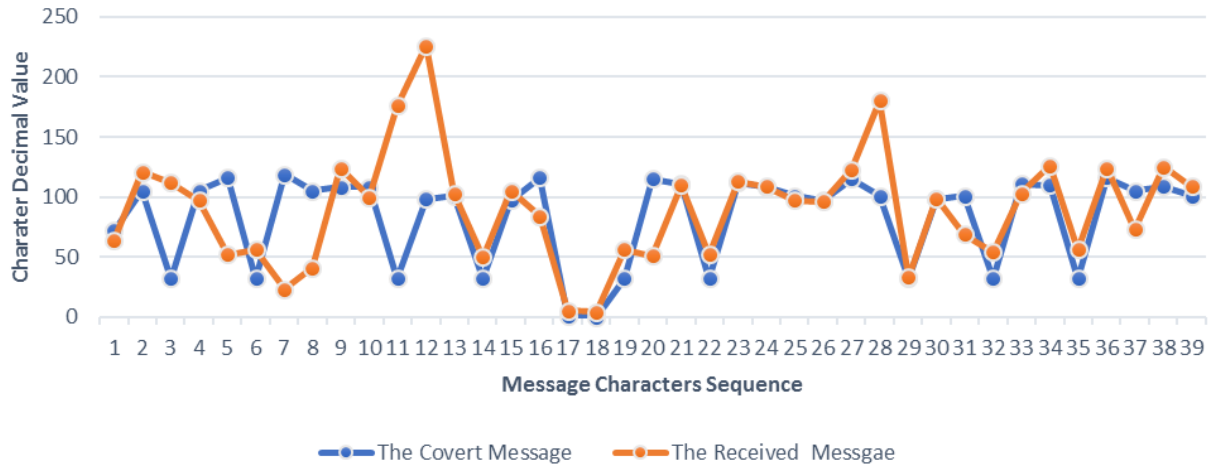

Figure 5. The Covert Message vs. the Modified Covert Message

9. Future Work

Our future work would be focused in verifying the capability of our proposed approach to counter other types of packet length-based covert channels. Theoretically this approach is sufficient to counter all other packet-length techniques. In addition, extra evaluation would be obtained using semantic similarity algorithms. Interested readers in semantic similarity are referred to the studies [34-38] for more information.

References

[1] B. W. Lampson, "A note on the confinement problem", *Communications of the ACM*, vol. 16, no. 10, pp. 613-615, 1973.

[2] L. Zhang, G. Liu, Y. Dai, "Network packet length covert channel based on empirical distribution function", *Journal of Networks*, vol. 9, no. 6, pp. 1440-1446, 2014.

[3] X. Lu, L. Huang, W. Yang, Y. Shen, "Concealed in the Internet: A Novel Covert Channel with Normal Traffic Imitating", in *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, pp. 285-292, 2016.

[4] M. A. Elsadig, Y. A. Fadlalla, "Survey on Covert Storage Channel in Computer Network Protocols: Detection and Mitigation Techniques", pp. 79-85.

[5] M. Elsadig, Y. Fadlalla, "Survey on Covert Storage Channel in Computer Network Protocols: Detection and Mitigation Techniques", *International Journal of Advances in Computer Networks and Its Security*, vol. 6, no. 3, pp. 11-17, 2016.

[6] M. A. Elsadig, Y. A. Fadlalla, "Network Protocol Covert Channels: Countermeasures Techniques", in *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, Manama, Bahrain, pp. 706-714, 2017.

[7] M. A. Elsadig, Y. A. Fadlalla, "An efficient Approach to Resolving Packet Length Covert Channels", in *6th International Conference on Computer Engineering and Mathematical Sciences*, Lankawi, Malaysia, 2017.

[8] R. DeGraaf, J. Aycock, M. Jacobson Jr, "Improved port knocking with strong authentication", in *21st Annual Computer Security Applications Conference*, , p. 10, IEEE, 2005.

[9] H. Qu, Q. Cheng, E. Yaprak, "Using Covert Channel to Resist DoS attacks in WLAN", in *ICWN*, pp. 38-44, 2005.

[10] W. Mazurczyk, Z. Kotulski, "New security and control protocol for VoIP based on steganography and digital watermarking", *arXiv preprint cs/0602042*, 2006.

[11] D. D. Dhobale, V. R. Ghorpade, B. S. Patil, S. B. Patil, "Steganography by hiding data in TCP/IP headers", in *3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, vol. 4, pp. V4-61-V4-65, 2010.

[12] H. Xie, J. Zhao, "A lightweight identity authentication method by exploiting network covert channel", *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1038-1047, 2015.

[13] G. J. Simmons, "The prisoners' problem and the subliminal channel", in *Advances in Cryptology*, pp. 51-67, Springer, 1984.

[14] J. P. Black, "Techniques of network steganography and covert channels", Faculty of San Diego State University, 2013.

[15] T. G. Handel, M. T. Sandford II, "Hiding data in the OSI network model", in *Information Hiding*, pp. 23-38, Springer, 1996.

[16] D. J. Dye, "Bandwidth and detection of packet length covert channels", Monterey, California. Naval Postgraduate School, 2011.

[17] M. A. Padlipsky, D. W. Snow, P. A. Karger, "Limitations of end-to-end encryption in secure computer networks: Technical report ESD-TR-78-158", *Massachusetts: The MITRE Corporation*, 1978.

[18] C. G. Girling, "Covert Channels in LAN's", *IEEE Transactions on software engineering*, vol. 13, no. 2, pp. 292-296, 1987.

[19] A. Epishkina, K. Kogos, "Covert Channels Parameters Evaluation Using the Information Theory Statements", in *5th International Conference on IT Convergence and Security (ICITCS)*, , pp. 1-5, 2015.

[20] Q.-z. YAO, P. ZHANG, "Coverting channel based on packet length", *Computer engineering*, vol. 34, no. 3, pp. 183-185, 2008.

[21] L. Ji, W. Jiang, B. Dai, X. Niu, "A novel covert channel based on length of messages", in *2009 International Symposium on Information Engineering and Electronic Commerce*, pp. 551-554, 2009.

[22] A. S. Nair, A. Sur, S. Nandi, "Detection of Packet Length Based Network Steganography", in *2010 International Conference on Multimedia Information Networking and Security*, pp. 574-578, 2010.

[23] L. Ji, H. Liang, Y. Song, X. Niu, "A normal-traffic network covert channel", in *International Conference on Computational Intelligence and Security, 2009. CIS'09.*, vol. 1, pp. 499-503, 2009.

[24] M. Hussain, M. Hussain, "A high bandwidth covert channel in network protocol", in *Information and Communication Technologies (ICICT), 2011 International Conference on*, pp. 1-6, 2011.

[25] A. Epishkina, K. Kogos, "A random traffic padding to limit packet size covert channels", in *Federated Conference on Computer Science and Information Systems (FedCSIS)*, pp. 1107-1111, 2015.

[26] O. I. Abdullaziz, V. T. Goh, H. C. Ling, K. Wong, "Network packet payload parity based steganography", in *2013 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (CSUDET)*, pp. 56-59, 2013.

[27] W. H. Gomaa, A. A. Fahmy, "A survey of text similarity approaches", *International Journal of Computer Applications*, vol. 68, no. 13, pp. 13-18, 2013.

[28] C. E. Akbaş, O. Günay, K. Taşdemir, A. E. Çetin, "Energy efficient cosine similarity measures according to a convex cost function", *Signal, Image and Video Processing*, vol. 11, no. 2, pp. 349-356, 2017.

[29] D. Lin, "An information-theoretic definition of similarity", in *ICML '98 Proceedings of the Fifteenth International Conference on Machine Learning*, pp. 296-304, 1998.

[30] W. B. Frakes, R. Baeza-Yates, *Information retrieval: Data structures & algorithms*. prentice Hall Englewood Cliffs, New Jersey, 1992.

[31] M. A. Elsadig, Y. A. Fadlalla, "Performance Analysis of Popular MANET Protocols", in *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, Manama, Bahrain, pp. 1085-1089, 2017.

[32] M. A. Elsadig, Y. A. Fadlalla, "Mobile Ad Hoc Network Routing Protocols: Performance Evaluation and Assessment", *Int. J. Com. Dig. Sys.*, vol. 7, no. 1, pp. 59-66, 2018.

[33] M. A. Elsadig, Y. A. Fadlalla, "VANETs Security Issues and Challenges: A Survey", *Indian Journal of Science and Technology*, vol. 9, no. 28, pp. 3-8, 2016.

[34] M. Abdelmagid, A. Ahmed, M. Himmat, "Information Extraction Methods and Extraction Techniques in the Chemical Document's Contents: Survey", *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 3, pp. 1068-1073, 2015.

[35] V. Rus, M. Lintean, R. Banjade, N. Niraula, D. Stefanescu, "Semilar: The semantic similarity toolkit",

in *ACL 2013 Demo Track*, At Sofia, Bulgaria, pp. 163-168, 2013.

[36] M. Abdelmagid, M. Himmat, A. Ahmed, R. KANNAN , "Survey On Information Extraction From Chemical Compound Literatures: Techniques And Challenges", *Journal of Theoretical and Applied Information Technology*, vol. 67, no. 2, pp. 284-289, 2014.

[37] S. Harispe, S. Ranwez, S. Janaqi, J. Montmain, "The semantic measures library and toolkit: fast computation of semantic similarity and relatedness using biomedical ontologies", *Bioinformatics*, vol. 30, no. 5, pp. 740-742, 2013.

[38] C. Gu, H. Xu, H. Zhou, J. Zhang, "Text similarity computing based on lexical semantic information", *Appl. Res. Comput*, vol. 35, no. 2, 2018.