Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.4, No.5, 2013

Capacity boost with data security in Network Protocol Covert Channel

Sujata Edekar
Computer Department, Pune University, MAE Alandi,
University of Pune 411015,
Maharashtra India
sujata.edekar@gmail.com

Prof. Rajeswari Goudar
Computer Department, Pune University, MAE Alandi,
University of Pune 411015,
Maharashtra India
rmgoudar66@gmail.com

The research is financed by Asian Development Bank. No. 2006-A171(Sponsoring information)

Abstract

Covert channels leaks information where information travels unnoticed i.e. the communication itself is hidden. Encryption used to protect the communication from being decoded by unauthorized users. But covert channels hide the existence of communication. Covert channels are serious security threat. There are many existing techniques available for development of covert channels by manipulating certain fields in the network protocols such as HTTP, IP, TCP, etc. The available packet length based covert channels are having tamper resistance capability but due to abnormal traffic distribution results in detection possibility. In this paper we present packet length based covert channel by using real time packet lengths where statistical detection of the covert channels is not possible due to random transformations and computations used in the algorithm. Also we improved the covert data capacity and security by applying certain encryption algorithm which doesn't change the length of the original data load compared to other available techniques. We focused on implementation details and try to find out the future expansion.

Keywords: Covert channels, packet length, high bandwidth, network protocols, packet payload, computer network

1. INTRODUCTION

Computer networks are a vital part of our lives. The different fields like educational system, commerce, banking organizations, industry, military everywhere we witness the manifestation of computer networks. Computer networks is linking tool for communication and association of information. Due to exposed information security facets of information is indispensable. Information Security has now become everyone's prerequisite, either directly or indirectly associated with network environs. The information may include the share market values, the database of the company, the quotations; military secrete data, and so on. So basically the information can be video, audio or in text form. The transfer of information is done by gmail, rediffmail such applications for mailing and for video conferencing Skype like applications are used. But due to this the need of information or the data security also increased in proportion to the data.

There are many techniques that are present in the market and explained in the academia also for the secure communication. Different cryptographic algorithms, data hiding techniques are used for information security. Encryption can just oppose the unauthorized access by third party. Compared to this covert channels data hiding techniques are used for hiding the presence of the communication [6]. The covert channels are a great threat to information security as the communication is carried out undetected[11].The covert channels utilizes information transmission free of charge[10].The performance of the system and the network get affected due to the hidden and unclear (may be illegal) use of resources or functions of the covert channel.

2. RELATED WORK

All Covert channels are used for confidential data communication during transmission. Lampson focused on covert channels and represented the concept firstly in 1973[1].According to him covert channels are divided into storage, legitimate and covert categories. Covert channels are also classified as storage and timing channels [13, 19].There are many techniques based on covert channels. But there are many factors like delay measurement, network conditions, congestion, traffic load etc. Due to which timing channels are may get affected by noise. So we are basically considering storage channels. There are many techniques available which utilizes packet header unused or reserved bits as covert channels.Ahasan[5] introduced IP's Don't fragment bit as covert channel whereas Sebastian Zander[11] used IP protocol's TTL field .TTL fields in IPv6 are referenced in [14,16,17]

Many other innovative and impressive techniques are also available like RSTEG [8] and CLACK [12].Concept wise the [8] is very effective strategy but real time implementation of RSTEG is difficult. There are four scenarios discussed [8].But [8] depends on many factors such as details of communication protocols, size of payload, rate of segmentation etc. So practical implementation for huge network is not possible. Whereas advantage wise the scenario 4 discussed in [8] is hard to detect, scenario 1 is easy to implement. There are certain constraints also for RSTEG like it should use the RTO -based retransmission. If RSTEG used with TCP protocol the chances of detections are more.

Sending data in the ACK field of the packet is another different concept, presented in CLACK [12].Its implemented via TCP data channel. According to author [12] CLACK is reliable and resilient in adverse network conditions and difficult to detect. In this [12] model the encoder is TCP receiver and decoder is sender. The requirement is that direct encoding is not possible. The partial encoding is used in this. The Nagale algorithm is turned off is the requirement of the model. So by assuming this condition the CLACK is designed.

There are specific models which uses the packet length for designing the covert channels. The base idea of our proposed system is also packet length and payload. Link layer frame length utilization for hidden communication is proposed by Padlipsky [7] and Girling [3].In this [3, 7] link layer frame length is mapped to each byte of covert message. So ultimately at least 256 message lengths are needed for single hidden byte. Predefined message lengths are used by sender and receiver. The main disadvantage of this system is the communication is detectable due to the statistical computations. The reason is due to predefined length (not real time) abnormal (not real) network traffic distribution.

LAWB model was proposed by Yao [18] in 2008.But due to abnormal traffic it's vulnerable to detection. Like our proposed model sender and receiver has shared a secrete matrix. The matrix is filled with unique packet length L .For sending a message sender selects a row ID as a covert message, and from the matrix selects a random cell in that row denoted by Len. When the packet arrives at receiver end it checks for the rowid of the cell in which the L contains. Periodic matrix transformation at both the sides is implemented by the author [18].

One more packet length based algorithm is introduced by Liping and Ji [9] in which the model is based on normal traffic distribution. As a Reference normal packet lengths from the network are captured from both ends of the system. The packet length to be transmitted is randomly selected from the list of Reference as well as the length for the next packet is generated by adding the covert message and send to the receiver. The reference list is modified by the sender when the packet sending is over. After arrival of the packet at receiver end, it extracts the covert data from the packet length received with the help of Reference list. The major drawback of this system is the newly generated packet length sometimes doesn't fit in normal length traffic distribution which results in detection of covert communication.

In the next paper of Liping Ji [15], he introduced Normal Traffic Network Covert channel. In this the real time packet lengths are taken as a Reference in sorted order. Equal size of buckets with specific packet length range is arranged. While sending the data sender select the group of covert bits and convert them into equivalent decimal. By selecting the equivalent decimal bucket with reference to packet length list, sender randomly selects the packet length from the bucket and sends it to receiver. At receiver end, checks for packet length and search into reference bucket range. If the bucket found the bucket number is nothing but the required covert data. This technique is utilizing normal packet lengths. The sender maintains the reference list at his end and receiver maintains the bucket ranges so the advantage of the technique is time and space efficiency. But if seen statistically then a pattern can be formed and detection is possible due to constant transmission which never gets updated. Also the covert data carrying capacity is low as compared to our technique.

3. PROPOSED MODEL

3.1 Terminologies

The proposed model is improved high bandwidth with improved security. It also sustains the tamper resistance and normal packet length distribution as stated in existing paper [2].It utilizes normal network communication

messages for referencing the length of the packet. Even though our model uses TCP protocol for implementation, we can also apply the same technique on different network protocols and achieve hybrid effect as future work. The main advantage of using the real time packet length is for achieving undetected data transmission due to normal traffic distribution. Packet length based methods are important with respect to the quality of attack resistant. Liping [9] and M Hussain [2] also proposed covert channels with normal distribution of packet in the network traffic. But our approach is based on improved security as well as improved bandwidth. In the proposed model we are using three main and standard characters for explaining the functionality of the algorithm

1. Alice, the secrete message sender

2. Bob, the message receiver

3. Warden, who try to capture the packets but unable to interpret the packet data due to unavailability of the Matrix.

Before starting for the communication Alice and Bob need to create a reference R x C dimensional master matrix on both sides, where each cell of the matrix is filled with real network packet lengths. Each cell is represents a unique length 'L'. R, C (rows and columns) of matrix is already known by Alice and Bob.

$\mathbf{CD=cd_0+cd_1+cd_2……cd_K}$, CD is the covert data bits and k is maximum number of bits in Cover Data

Further the CD is divided into Subgroup of W bits.

$\mathbf{CD=W_i+W_{i+1}……W_{i+q-1}}$,Where Wi be the ith subgroup of C where q is the maximum length of subgroups of CD ,i is the counter and Wd is the decimal value of Wi.

V is the (covert) steganos-column of matrix

Y is the (covert) stego row of matrix

3.2 Algorithm

Step 1: At first synchronization is carried out. In this Alice (Sender) and Bob (Receiver) filled the R x C matrix in predefined order with the normal or real network traffic packet lengths.

Step 2: Alice selects Wi, the ith subgroup of CD, and converts it into decimal Wd value. Find the equivalent Wd row ID into matrix and randomly select a cell in that row. So, a packet length denoted as Len is retrieved.

Step 3: If the column, row of selected cell is matched to V (stego) and Y (stego row) send normal packet of 'L' size.

Step 4: Else If the column of selected cell is matched to V (stego column), which indicate that sender will send the covert data of 'L' size in the payload of that packet in encrypted form.

Step 5 :Else If column of selected cell is matched to Y (stego row), which indicate that sender will send the covert data in rowid + next 'L' size data in the payload of that packet in encrypted form

Step 6: If Step 5 fails then, Sender sends the normal data packet in encrypted form of 'L' size to the receiver.

Step 7: Receiver simply find out in his matrix a cell which contain the equivalent size of the received packet length.

Step 8: If the column, row of selected cell is matched to V & Y Receiver discard the packet.

Step 9: Else If the column of the selected cell is matched to V then extract data directly from the packet payload.

Step 10: Else If the row of selected cell is matched with Y then form the covert data by appending decrypted payload next to rowid.

Step 11: If Step 10 fails, then Stego data is extracted by the row ID of the selected cell.

Step 12: After each packet transmission, both Alice and Bob reshuffles their matrix in predefined order.

Step 13: Above steps repeat until the Alice has covert data to send.

When applied a standard encryption algorithm the actual length of the packet changes, but the model depend on packet length and this may cause to crash the application. So instead of standard encryption we used the randomly generated stego row for encryption of the data. This will results in randomization, so this technique is based on NP Hard.

Now from the algorithm we can conclude that the scheme is used for capacity improvement over the existing systems. We are using payload and packet length fields for covert communication. Here the length is indirectly utilized for extracting the rowid i.e. the hidden w bits of the message. Moreover the lengths in the matrix are unique as well as captured from real traffic network. So it's pretended to be normal communication through normal traffic distribution so the sending is safe and undetected.

In previous system fixed T packet transactions, as T is fixed either as time or as number of packets. But we eliminated this possibility by introducing new terms like random stego row. With the help of mathematical computation we generate the random numbers for transforming the matrix. So statistical detection is not possible in this case. Every element in the matrix is not having any direct relationship with neighboring element. So the system by maintaining the benefits of the existing system is efficient for both homogeneous as well as heterogeneous data [2].

3.3 System Architecture

The flow of information is as shown in the figure 1 .As discussed stego column ,number of rows and columns are shared between the communication parties with any secure communication medium[4].The mediator can be any router or any in between node, who tries to interpret or capture the data. AS the matrix is not available with the third party the interpretation of the data is impossible. The data travels from sender through the network reaches to receiver. And the acknowledgment is send to sender. The flow is as shown in the figure 1.

By set theory the definition of System 'S' can be given as **S={Mat,R,C,CD,W,V,Y,L,Msg}** in which Msg is the message to be send ,CD is divided binary data ,and L is length of the message and rest of the things are as defined in the algorithm of the proposed system. The detailed working MODELS of the system is as shown by the system architecture diagram in the figure 2.

4. CONCLUSION

Now from the algorithm we can conclude that the scheme is used for capacity improvement over the existing systems. We are using payload and packet length fields for covert communication.

In the proposed technique sending is safe and undetected. In previous system [2] T is fixed either as time or as number of packets. But we eliminated this possibility by introducing new terms like stego row. With the help of computation depending on the random values of stego row we transform the matrix. So statistical detection is not possible in this case, due to independent existence of every element in the matrix. So the system by maintaining the benefits of the existing system is efficient for both homogeneous data as well as for the heterogeneous data [2].

As a future work the combination of different network protocols can also be used as hybrid model. In this case again in a random fashion we can utilize the protocols and rearrange the message at the receiver side. We can also increase the bandwidth utilization by applying the CLACK [12] at receiver end, so that the communication will be bidirectional.

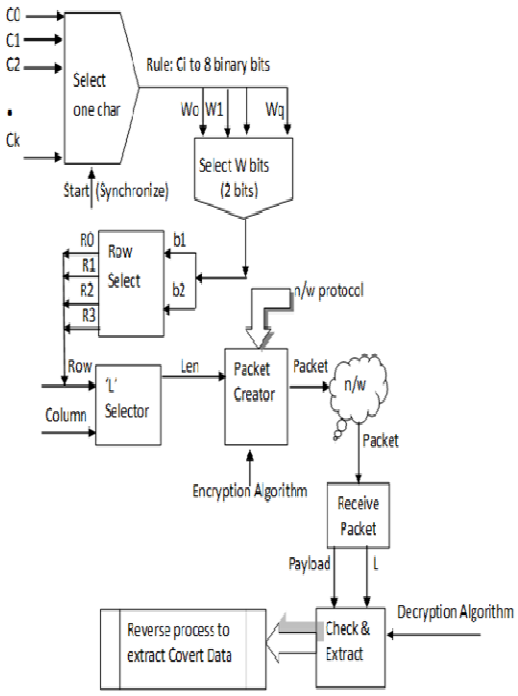

Fig 1. System Flow Model

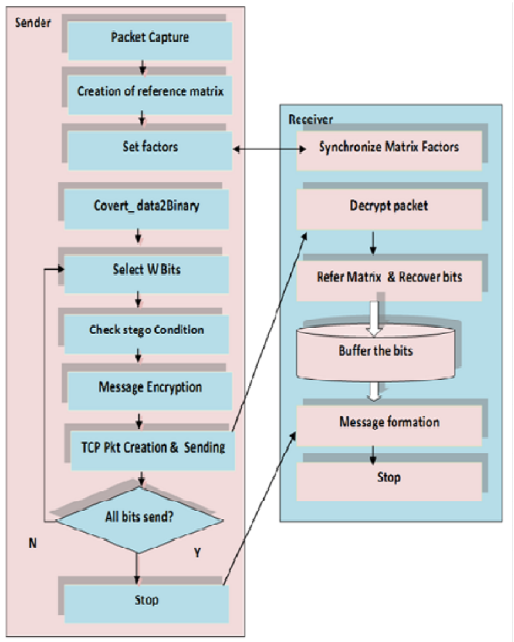

Fig 2 :System Architecture

5. REFERENCES

B. Lampson. A note on the confinement problem.Communications of the ACM, 16(10) : 613 - 615, October 1973.

Mehdi Hussain,M.Hussain ,"High Bandwidth covert Channeslin network protocol",IEEE Computer ,2011

C. G. Girling, "Covert channels in LAN's", IEEE Trans.Software Engineering , vol. SE-13, no. 2, pp.292-96, Feb. 1987.

W. Stallins,"Applied Cryptography",McGraw hill

K. Ahsan, D. Kundur, "Practical data hiding in TCP/IP",ACM Workshop on Multimedia Security, December 2002.

Cai Zhiyong,Shen Ying,Shen Changxiang ,"Detection of Insertional Covert Channels Using Chi-Square Test",IEEE ,2009

M. A. Padlipsky, D. W. Snow, and P. A. Karger,"Limitations of end to -end encryption in secure computer networks", Tech. Rep. ESD-TR-78-158, MitreCorporation, August 1978

Mazurczyk W., Smolarczyk S., Szczypiorski K.,"Hiding Information in Retransmissions",In Computing Research Repository (CoRR),abs/0905.0363, arXiv.org E-print Archive,Cornell University, Ithaca,NY (USA), May 2009.

Liping Ji, Wenhao Jiang, and Benyang Dai,"A novel covert channel based on length of messages", International Conference on e-Business and Information System Security, 2009.

D. Gries and F. Schenider. A Logical Approach to Discrete Math. Springer Texts And Monographs In Computer Science. Springer-Verlag, New York, 1993.

Sebastian Zander, Gernville Armitage, and Philip Branch,"A Survey of Covert Channel and Countermeasures in Computer Network Protocols", IEEE Communications Surveys and Tutorials, vol 9, no.3, pp. 44-57, 3rd Quarter 2007.

Xiapu Luo Chan, E.W.W. Chang, R.K.C"CLACK:A Network Covert Channel Based on Partial Acknowledgment Encoding". ICC'09. IEEE International Conference on 14-18 June 2009.

Pukhraj, Singh. Whispers on the Wire, Network Based Covert Channels,White paper,gray-world.net/papers/pukhrajsingh covert.doc

Zander, Sebastian. Grenville, Armitage, Philip Branch." Covert Channels in the IP Time To Live field", Center for Advanced Internet Architectures (CAIA), Swinburne University of Technology, Melbourne,Australia

Liping Ji, Haijin Liang, Yitao Song, Xizmu Niu,"A Normal Traffic Network Covert Channe", Computational Intelligence and Security,2009.

T. Handel and M. Sandford, "Hiding Data in the OSI Network Model" ,Proc. 1st IntâAZl. Wksp. Information Hiding, 1996 pp. 23 âAS 38.

C. Abad,"IP Checksum Covert Channels and Selected Hash Collision",tech. rep., UCLA, 2001.

YAO Quan-zhu and ZHANG Peng, "Coverting channel based on packet length", vol.34 No.3 Computer Engineering, February 2008.

U.S. Department of Defense. Trusted Computer System Evaluation "The Orange Book " Publication DoD 5200.28-STD. Washington : GPO 1985 , http :// www.radium.ncsc.mi l/ tpep/ library/ rainbow/ 5200.28-STD.html