ISSN 2277-3061

Secure SDN Frameworkfor Data Exfiltration via Video Steganography

Shantala C.P, K.V Viswanatha
Research Scholar, C.M.R University, Bangalore, Karnataka, India
shantala.14phd@cmr.edu.in,
Research Guide, C.M.R University, Bangalore, Karnataka, India
viswnathakv@yahoo.com

ABSTRACT

The popularity of steganography in the data exfiltration of private corporate sensitive data is increased. So it is important to detect such malicious activity. Becausethe data being transferred can hide the large amount of data in video becoming increasingly attractive. To ensure privacy and security we proposed an effective steganalysis method to detect hidden data in video by using the SDN framework policy. The main objective of this paper is to prevent the illegal data transmission from the compromised private network by the malicious users.

Index Terms

Steganography, Data exfiltration, and Software defined network.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol. 14, No. 9
www.ijctonline.com, editorijctonline@gmail.com

INTRODUCTION

Securing the sensitive data from both outsiders and also from insider is a biggest challenge in the private corporate network. Data exfiltration [1] is the illegal copying, transfer or retrieval of data from a computer. Data exfiltration is a malicious activity performed through various different techniques, typically by cybercriminals over the Internet or other network.Because of data exfiltration attacker can seal the sensitive information in the private network.

To prevent data exfiltration [2], administrators should create strict IT controls for both physical and digital security. Identifying anomalies in the data exfiltration is critical to know and to spot the insider attacker. The insider has the typical lifestyle a) Identify places where sensitive data is stored b)Retrieve the data from the location c)Move the data within the organization to prepare for exfiltration d)Transfer the data outside the organization.

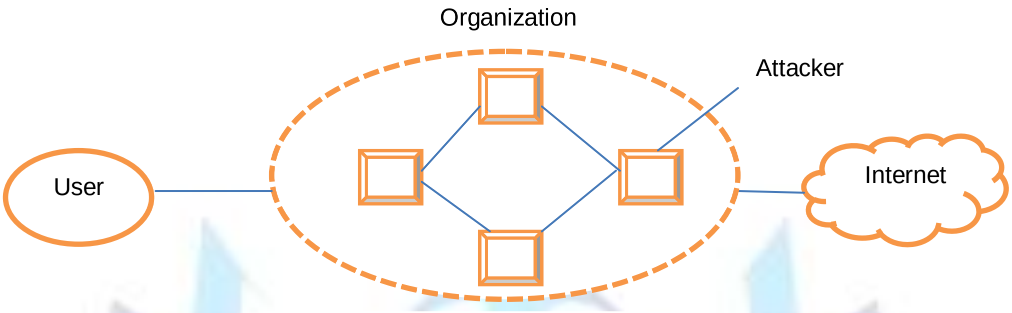


Fig 1: Data Exfiltration

A new technique for data exfiltration has been seen in the world using video uploaded to cloud services as a way to move data out of compromised networks without detection. The technique utilizessteganography [3] where encrypted new data is encoded into video files and uploaded to semi trusted or unmonitored video sharing services.

Steganography encompasses all concealing techniques that embed a secret sensitive message into carrier of the message in such a way that the carrier modification caused by the embedding of steganogram must not be noticeable to anyone.

In this paper we address the problems for the new method of data exfiltration and also propose SDN framework to detect and overcome the problems of data exfiltration with video steganography.

THREAT MODEL

A new method of data exfiltration is found with video steganography [4], attacker transfer the data from private network to outside network without detected by the administrator of the private network. Why only videos not images? – Security experts know that there are several tools available that can use of steganography in images, but not in videos and large amount of data cannot be hidden in images[9] ,in audio steganography due to channel noise data will be destroyed [10] and in text steganography hidden message can be destroyed easily [11].

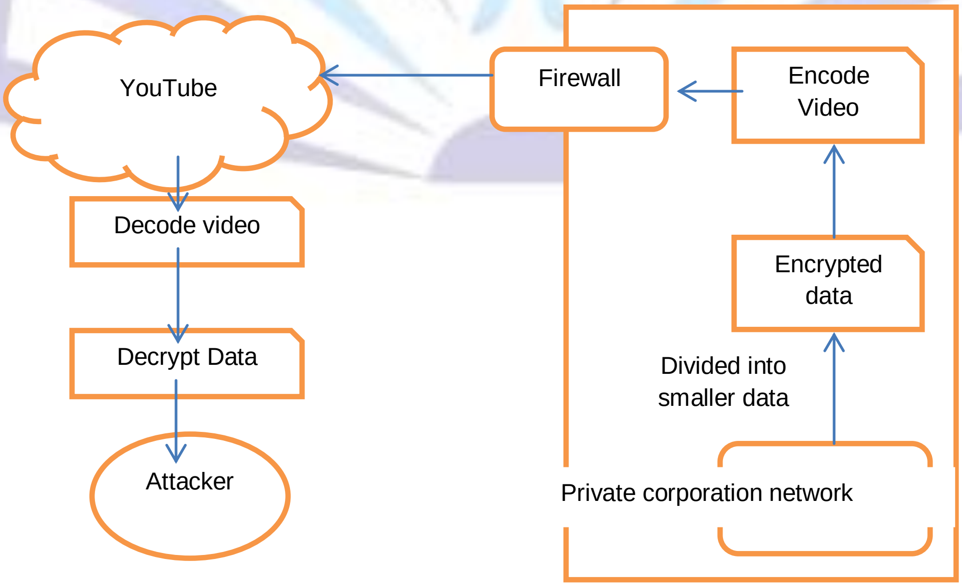


Fig 2: Data exfiltration using video

The Fig 2 shows typical threat model, data exfiltration's are targeted attacks where the hacker's/crackers primary intent is to find and copy specific data from the target machine. The hackers/crackers gain access to the target machine through a remote application or by directly installing a portable media device. Then attackers divide the data with equal parts and then encrypt the data later applying steganography method like embedding the encrypted data into videos.

Later he upload the video into cloud based video sharing services like YouTube [5], this leads data theft from the private corporate. This method of data theft leads a serious issue in the compromised network. Identifying the transmission of this kind of exfiltration is very difficult. In this proposed system we are going to propose SDN framework for detecting and preventing the video steganography.

PROPOSED SYSTEM

In this paper, we propose a new SDN security framework for detecting and preventing the data exfiltration with the help of video steganalysis.

A). SDN-based forensic system

SDN [12] separates the network plane into control plane and data plane, and that control plane is programmable and increases flexibility.SDN requires some method or interface for control plane to communication with data plane One such mechanism is called as OpenFlow protocols [13]. Because of this higher level software to configure the control plane of network packets on demand, priority based packet forwarding enables the infrastructure to quickly adapt new application requirements. The following figure shows the SDN architecture.

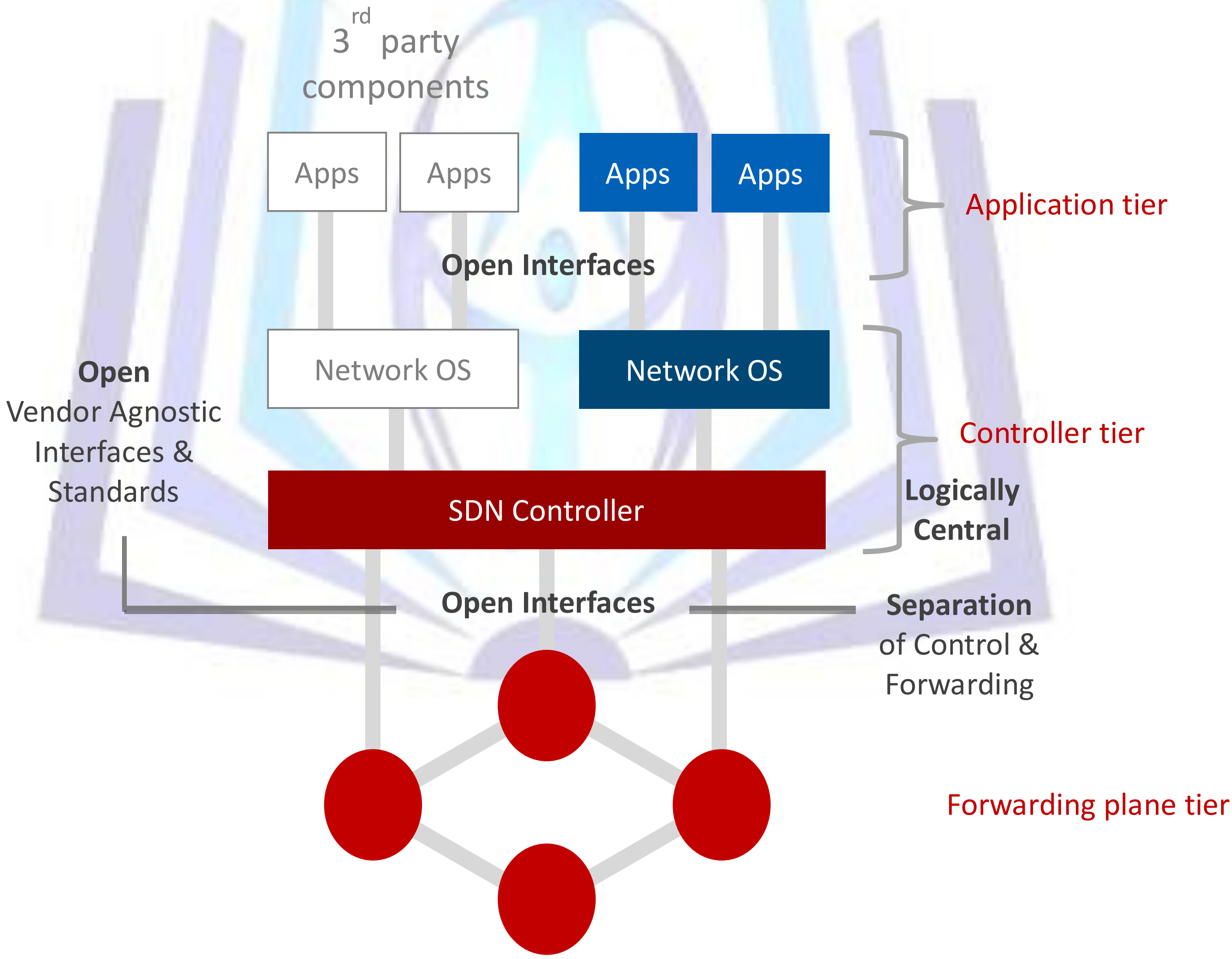


Fig3:SDN architecture

OpenFlowis a communications protocol that gives access to the forwarding plane of a network switch or router over the network. OpenFlow enables remote controllers to determine the path of network packets through the network of switches

It is very difficult to observe the network host systems behavior by administrator in traditional network system, since these compromised systems may use duplicity or alter with data to disturb forensic analysis.

Within the constraint of corporate network, network provenance can be used to trace back traffic and discover the cause of an event. Example, an administrator can use a network provenance system to discover if a suspicious routing table entry is due to simple configuration.

Network provenance systems have been applied in distributed systems to detect faults and attacks while incurring only modest overheads. These systems often rely on correct nodes to observe and record the actions of other nodes for possible forensic uses. Limitation of this approach is that, if an attacker carefully avoids interacting with nodes, he may remain invisible to forensic system.

This is problematic in private corporate network that are stored sensitive data, if these data are exfiltrated to a remote adversary like cloud video sharing services, the provenance system cannot identify the node that leaked the data unless the leakage was observed by at least one correct node.

Through the advent of software defined networking [6], we can use the network itself as the observation point of forensic system.System administrator is able to ascertain the correctness of every system when issuing a forensic query, making it possible to detect the presence of previously unobservable attacks.

Rather than rely on reports from end nodes, we can transform every network link into a reporting tool by programming a distributed set of SDN switches and middle boxes [7]. Accomplishing such a feat in traditional network system would have been costly and complicated, requiring a proxy boxes between every node in the network.Based on the set of programmable flow table rules, SDN allows us to perform complex sets of operations on a packet as it enters a switch. By pattern matching in the packet headers, these operations permit dropping unauthorized communication.

By adopting the software defined networking in the data exfiltration threat, administrator of the private network can observe the whole network in the laptop and he can control the network by programming.

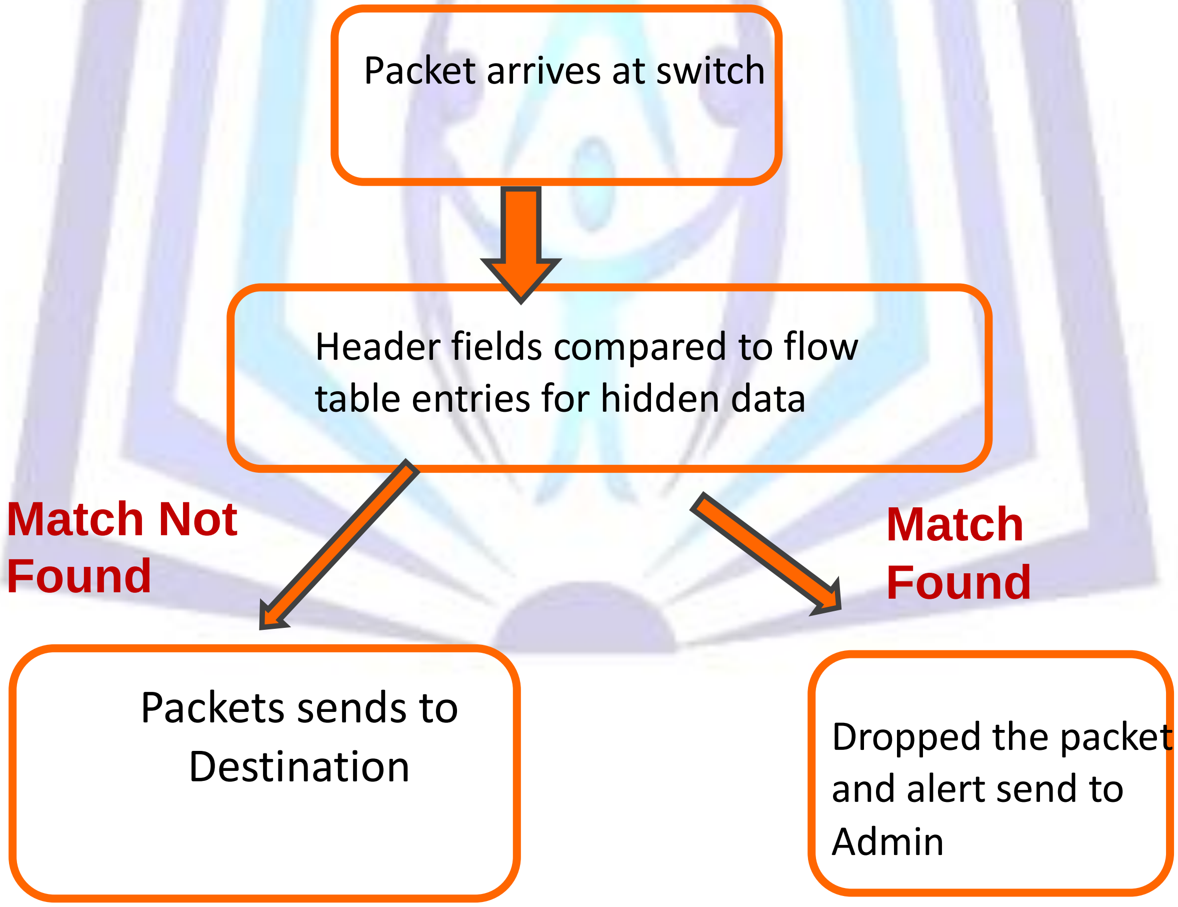

Packet arrives at switch
Header fields compared to flow table entries for hidden data
Match Not Found
Match Found
Packets sends to Destination
Dropped the packet and alert send to Admin

Fig 4: SDN based forensic system

As shown in the figure 4 whenever the packets arrives at the switch its header fields are compared to flow table entries to check whether there is a hidden data if match is found then packets are dropped and alert message will send to the admin. if there is no match then packets will sends to the destination.

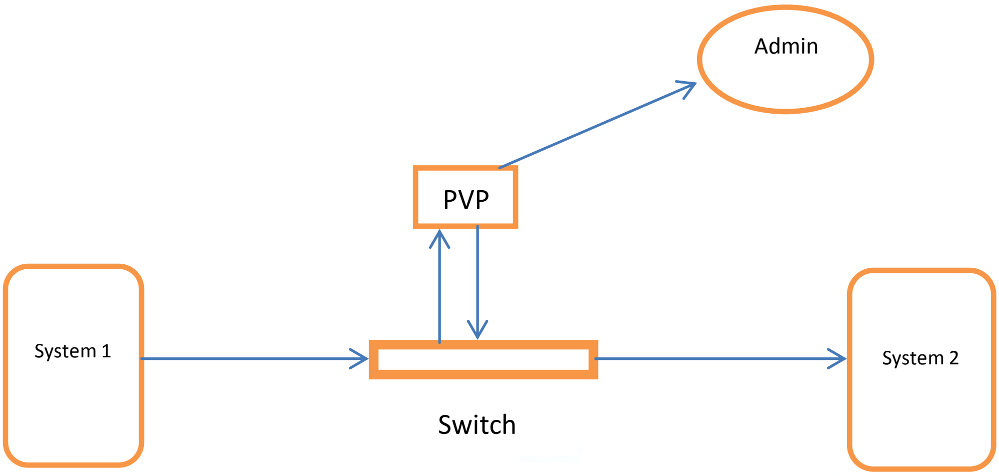


Fig 5: Provenance verification points

The above figure shows an SDN based forensic system, provenance verification points are middlebox components forensic packet processing.

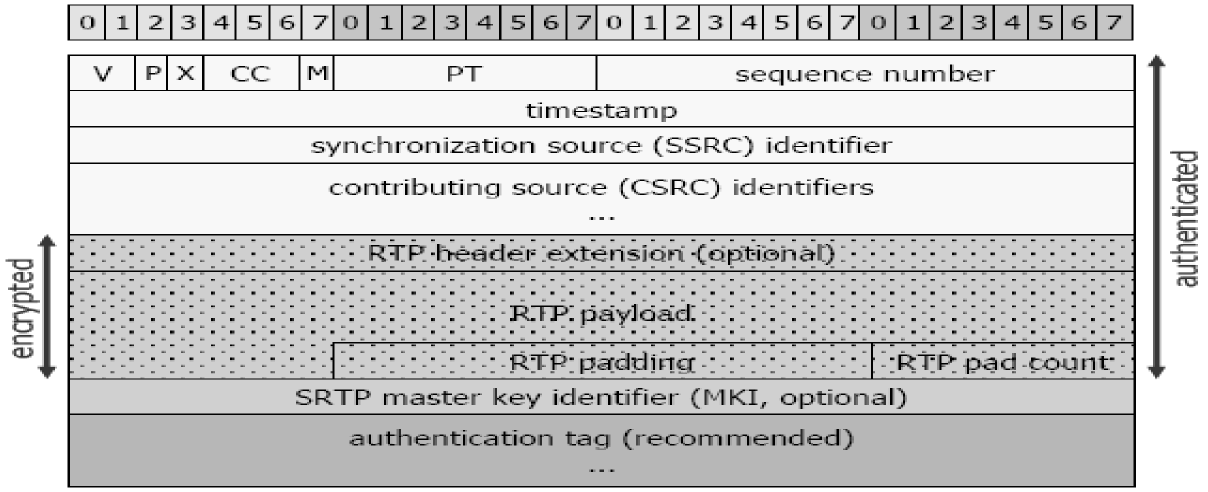
We assume that all inter node communication in the private network take place through the monitored network; communication via wireless technologies or sneakers is not possible. Similarly communication entering or leaving the private corporate network must pass through SDN switches.

The SDN functionality available on a switch is not sufficient to build a forensic system so we are using middleboxes provenance verification points. Each PVP is responsible for monitoring the activity for some system nodes.

PVP's actively enforce message commitment protocol, dropping the packets that contain malicious data (other than video), when PVP detects such type of message then it can alert the system administrator.

The main innovation of this method is to find a codec that will result in a similar video quality but smaller video payload than the originally selected. When the video stream is transcoded, the original video payload size is intentionally unaltered and the change of the codec is not indicated.After placing the transcoded video payload, the remaining free space is filled with hidden data.

So it is very difficult to find the hidden data communication for above mentioned method, with help auditing the payload field in the real time transport protocol(RTP) [8] header, administrator of the private network can identify the data exfiltration with video steganography.


0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
V
P
X
CC
M
PT
sequence number
timestamp
synchronization source (SSRC) identifier
contributing source (CSRC) identifiers
...
RTP header extension (optional)
RTP payload
RTP padding
RTP pad count
SRTP master key identifier (MKI, optional)
authentication tag (recommended)
...
encrypted
authenticated

RTP packets carrying user video are inspected and the codec originally used for video encoding (here called covert codec) is determining by analyzing the payload type field. Covert codec yields a comparable video quality but a smaller video payload size than original.

Next, the video stream is transcoded, but the original, large, video payload size and the codec type indicator are preserved, thus the PT field is left unchanged. Instead, after placing the transcoded video of a smaller size inside the original payload field, the remaining free space is filled with hidden data.

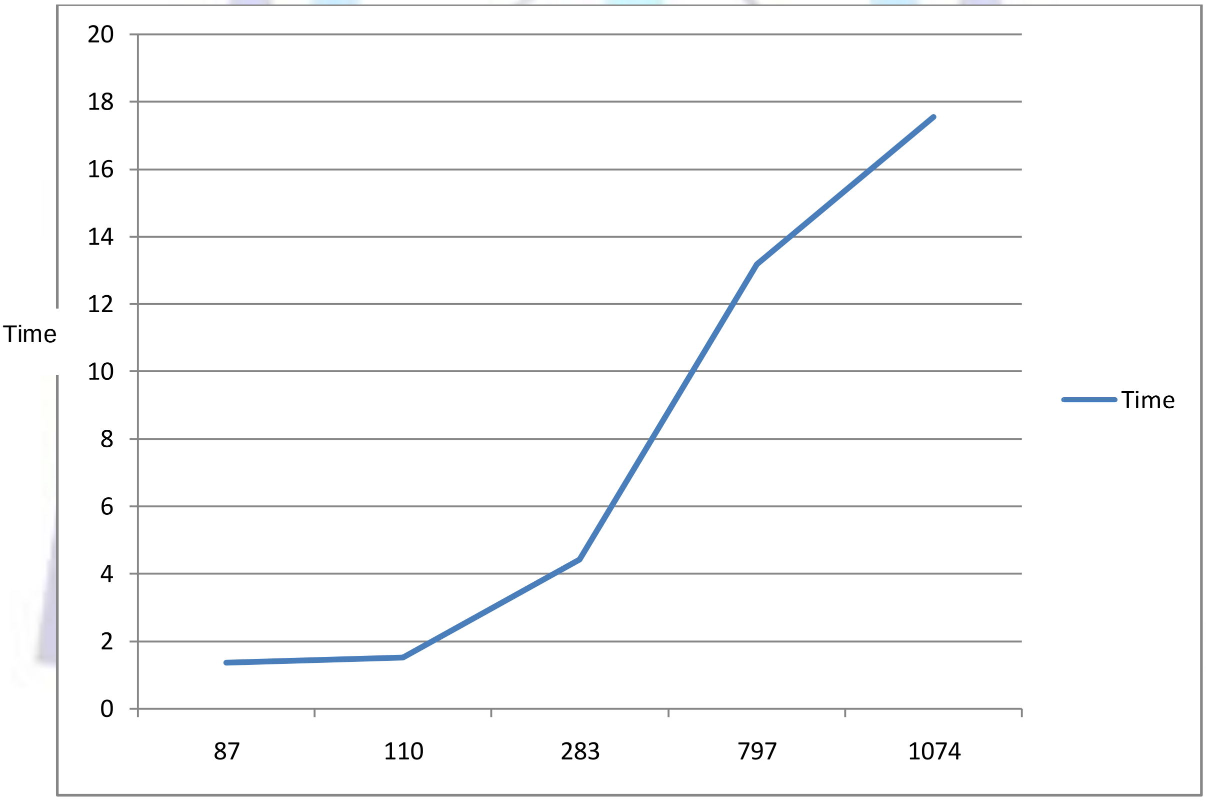
RESULTS

Results are analyzed for audio files of different sizes and the numbers of frames are calculated .If the size of the audio file is more then it will divide into large number of frames and takes more time. The audio files are added into the payload field in the packet. Results are tabulated as below:

Table 1. Analysis of results

Secret Audio file **Size**	**Number of frames**	**Time**
1.5 Mb	283	00:04:43.00
591 Kb	110	00:01:50.00
5.8 Mb	1074	00:17:54.00
4.3 Mb	797	00:13:17.00
453 Kb	87	00:01:35.00

When graph is plotted by taking number of frames in x axis and time in y axis the results will be as shown below:



Number of frames

Graph 1:Variation of time based on number of frames

Conclusion

In this paper, we have investigated the problem of data exfiltration with video steganography, which is very dangerous in private corporate network. To ensure the security of the sensitive data in compromised network we proposed an effective steganolysis strategy with double guard framework using the software defined networking and secure auditing system. Through thedetailed analysis, we have seen that our scheme almost guarantees the security of the sensitive data.

Future Enhancement

It is possible to detect video steganography only in some formats of videos .so it must be enhanced to detect in all video formats.

References

[1] Iftach Ian Amit, “Advanced Data Exfiltration–the wayQ would have done it”, iamit, September 2011.

[2]http://www.tripwire.com/state-of-security/incident-detection/hackers-exfiltrating-data-with-video-steganography-via-cloud-video-services/

[3] Shantala C P, K V Viswanatha, “Different Steganography Methods and Performance Analysis”, International Journal of Engineering Inventions, ISSN: 2278-7461, ISBN: 2319-6491, Volume 2, Issue 1 (January 2013) PP: 37-45.

[4] NatarajanMeghanathan and LopamudraNayak,“Steganalysis algorithms for detecting the hidden information in image, audio and video cover media”, International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010.

[5]https://www.youtube.com/

[6]ShridarK NRao,“SDNandItsUseCase-NVandNFV” NTIL2014.

[7] https://www.sdxcentral.com/resources/sdn/sdn-controllers/sdn-controllers-comprehensive-list/

[8]WojciechMazurczyk, PawełSzaga, Krzysztof Szczypiorski, “Using Transcoding for Hidden Communication in IP Telephony”,Multimedia Tools and ApplicationsJune 2014, Volume 70, Issue 3, pp 2139-2165.

[9] Sadoon Hussein Abdullah, “Steganography Methods and some application (The hidden Secret data in Image)”, April 2009.

[10]Jayaram P, Ranganatha H R, Anupama H S,” INFORMATION HIDING USING AUDIO

STEGANOGRAPHY – A SURVEY”, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.

[11] Monika Agarwal, “TEXT STEGANOGRAPHIC APPROACHES: A COMPARISON”, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013.

[12] Sandra Scott-Hayward, Gemma O’Callaghan and SakirSezer, “SDN Security: A Survey”.

[13] Wolfgang Braun * and Michael Menth,” Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices”, May 2014

About Author’s

Prof.Shantala C.P. received the B.E and M.Tech degrees both in computer science and engineering. She is working towards the Ph.D from C.M.R University. She is also serving as Vice principal & Head of the Department of Computer Science & Engineering, Chanabasaveshwara Institute of Technology, NH 206,BH road ,Gubbi,Tumkur,karnataka,India-572216.

Dr. K.V Viswanatha received B.E, M.Tech and Ph.D in IIsc, Bangalore. He is currently working as a Dean PG studies, Department of Computer Science & Engineering, Chanabasaveshwara Institute of Technology. NH 206,BH road ,Gubbi,Tumkur,karnataka,India-572216.