ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (141-151), Month: January - March 2016, Available at: www.researchpublish.com

A Survey on Traffic Analysis in Networks

[1]Saurav Mishra, [2]Manjusha Pandey, [3]Gargi Srivastava

[1, 2, 3] School of Computer Engineering, KIIT University, Bhubaneswar, India

Abstract: **Since last 20 years the network traffic analysis has increase largely over the couple of years. This was mostly due the increase in network access speeds, increasing of cyber-crime in the networks, Internet service protocol also increase. Due these interest is increase massively between the user towards the internet. Traffic is a flow of data across the Internet during the particular time. Traffic analysis is the process of intercepting and detect the message in order to deduct the information. Traffic analysis has been affected by attackers to threated user's privacy in the cyber world. So that there is different type attack are used to detect the traffic analysis are used. So, in this paper I survey on traffic analysis and focused on the different traffic attack, P2P proxy caching, virtue networks, and also focused on DDOS detection.**

Keywords: **Traffic analysis attack, Intrusion detection system, Peer to peer, wireless sensor network, false positive and negative, virtual vector, domain server name, Traffic analysis.**

1. INTRODUCTION

Since last 10 years the network traffic increase massively over the last couple of years. This was mostly due 1) The increase in network access speeds. 2)The increasing of cyber-crime in the networks .3) The ISPs' increased. Due these interest is increase large amount between the user towards the internet. [1]. The Internet is the global system of correlation computer networks that use the Internet protocol suite that is to link millions of devices worldwide area. The network traffic is link to different type of non- public sector, public places, offices, industrial propose. The Internet carries a large amount of information resources and services, such as different applications of the website, mail, telephonic information etc. Since last 15 years the traffic analysis is mostly attractive topic for the research point of view [2]. Traffic analysis is the process are to identify the message in order to deduct information from pattern in communication. Traffic analysis can have performed in the context of military intelligence, school or pattern-of-life analysis, and is a concern in computers security. Traffic analysis tasks may be supported by loyal computer software programs. The traffic analysis can perform med in the context counter measurement, intrusion detection system, and industrial networks. The malware infection based on the domain name server (DNS) and also performed on the P2P caching analysis. The traffic analysis Most pointed out in the peer-to-peer file sharing applications, which can be responsible for more than 95% of the total traffic volume depending on the location. There is different type of mechanisms which help in detection different type of attacker such as: 1) Dummy Source: This is some dummy traffic generation mechanisms where the getaway simulates the transmission of a fake sensor, hence it makes the attacker believe that is given a type of sensor is mounted on the patient. 2) Dummy Source: This is dummy traffic generation, where the getaway injects dummy message in a completely random manner, hence create a noise to cover the real traffic

1.1 Wireless Sensor Network in Traffic Analysis:

A wireless sensor network [3] is consisting of spatially different autonomous device using sensor node with sensing, communication, and phenomena in a special [4] environment for a various application. For the security concern problem as traffic analysis attacks because critical issue aroused the researcher point of view in wireless sensor network. Traffic analysis attack try to deduct the context information of node by analysis the traffic pattern form attacker on the wireless communication. Specification the attacker might arrange a lot of information about the network topology and deduct the location of the through observing the traffic volume and pattern. WSNs are used for a large number of place such as for

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (141-151), Month: January - March 2016, Available at: www.researchpublish.com

monitoring, industrial use networks health [5] monitoring, water efficiency [6]. The main advantage is that they are easily developed in large and harsh areas information is sense collected by battery-operating nodes and transmission through a multi-hops scheme to a central server knows a sink for the father processing. The WSNs become worldwide their security issue have become a major concern. Wireless sensor network faces a number of security threats at different layer such as jamming attack at the physical layer routing attack at the network layer

1.2 Intrusion Detection System:

Intrusion detection mean that it can detecting unwanted traffic on a network or advice [7]. There are several reasons that make intrusion detection is important part of the computer system. There are many traditional systems and applications were work without out the security. In other cases, systems and applications were developed and work in a different environment that may become harmful when deployed Intrusion detection complements these detection mechanisms to improve the system security. An intrusion detection system can be divided into two-part anomaly based and misuse detecting system. An anomaly based is also known as behaviour based system while misuse based system is knowledge based system.

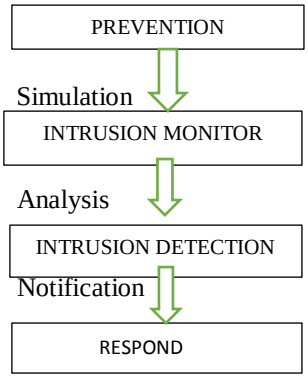

Figure 1: Flow Chart of IDS

The intrusion detection can be divided two type:

1.2.1 NIDS: The network intrusion detection system is an independent platform that identifies that intrusion by examining network traffic and monitors multiple host, developed in 1986 by peer. [8] Network intrusion detection system gain across access to network by connecting to network hub, network switch configuration for port monitoring or the network hop. Network based detection play a major role in traffic analysis.

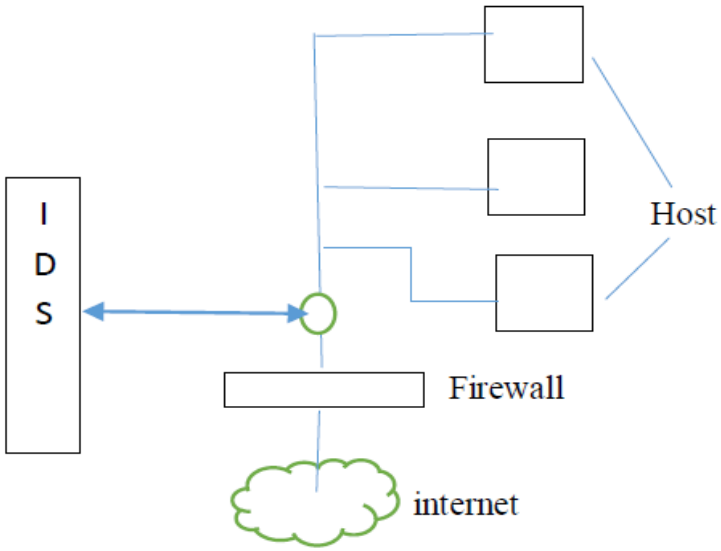

Figure 2 NIDS

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 1, pp: (141-151), Month: January - March 2016, Available at: www.researchpublish.com

1.2.2 HIDS: Host based detection system analysis network traffic [7], [8]and system-specific settings such as software cell, local security policy, local audits etc. A HIDS must be installed on each machine and required configuration specific on that operation system. The misuse of host based intrusion detection system.

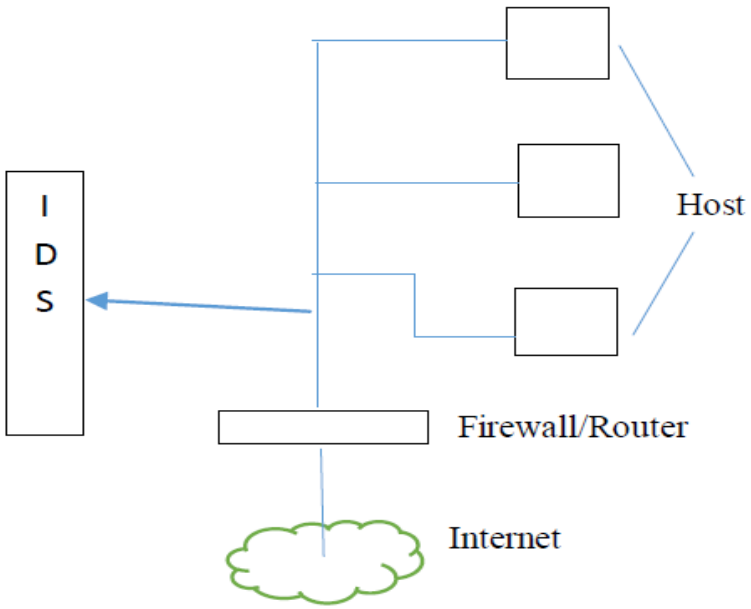

Figure 3 HIDS

1.3 Traffic Analysis Attack:

There is different type of traffic analysis attack, they as follow:

1.3.1 Passive Attack: A passive attack monitors unprotected traffic such as sensitive information, password, account no. These used to protect the necessary data that are used by the user in day to day life. Passive attack provides defence or security from the attacker.

1.3.2 Active Attack: In the cases of active attack, the attacker tries to break the security of system through virus. Active attacker includes malicious virus, steal and modify the data.

1.3.3 Password attack: In these cases, an attacker tries to find the password that is store in a network or host or I address of the user. By the help of the user data or password the attack tries to detect the important data the user store with it.

2. LITERATURE SURVEY

2.1-Data Analysis of false positive and false negative from Real traffic analysis with intrusion detection and intrusion prevention System:

In the year 2012 change-yuan ho,et.al. [9] proposed a mechanism for false positive and negative assessment with multiple IDS and IPS to collect false positive data from real-world traffic and statically analysis as the author had obtained the three fact More than 92.5% of false cases are Fps even if the number of allow types for false positive and false negative are similar About 94% of FP alert equal to about 85% of false cases are not related to security issue but not manage policy. The SQL server attacks and worm slammer attack account for 94% of false positive. The author had collects more than two thousand cases of False negative and false positive from the real-world traffic of campus bet site by the libpacp system, in order to observed what kind of false positive and false negative an happen easily in which protocol and what it kind of attack and investigate their frequencies across all false negative .The author had collected some following fact are, there is 13 times more false positive than there is FN although number of attack type in FN and FP are similar The Buffer overflow and SQL server attack and worm slammer attacks account for 94% of false negative. The network administration promptly while this not only execute what the IDS, but also the suspected malicious source. The FNs is much more serious than the FPs, because of negative effect of FNs which is used to reduce trust in intrusion detection system The signature –based detection is missing in both of case FP as well as the False negative. False positive and

negative are still the key issue for IDS and IPS which are less reliable today because of the limitation of the signature – based methodology. The author uses the FPNA mechanism in the PCAPLIB system to provide analytical analysis of false negative and false positive cases. FPNA collected more than three thousand of false negative and false positive The FPNA mechanism consist of three components as majority voting, trace verification and manual analysis. The author had uses the false positive and negative assessment with DUTs to trace different data form the FPFN mechanism to provide potential and efficiency by the used of intrusion detection and prevention system. By this technique the author can prolong the life of internet traffic.

2.2 On the assert of cooperative proxy caching for peer-to-peer traffic:

In the year of 2010 Mohamed hefted et.al [10] has proposed analysis a potential gain correlations proxy caching for different traffic as mean to ease the burden imposed by transforming one place to another traffic on internet service provider. The author had purposed a two model for correlations caching of peer to peer traffic. The first model enables a correlation among caching that belong to different auto mouse system. While the second consider correlation among caches developed within the same. The author had analysis the potential gain of cooperative caching in these two model. The author had performed extensive trace-based simulation to analysis different angle of correlation caching scheme, the author had uses the, Significant improvement in byte hit rate can be achieved by correlation caching. The Overhead imposed by correlation coaching is negligible. The author has used a caching algorithm based on segmentation and partial caching of the object. They also design and implement protocols for a proxy cache for peer to peer traffic. The author has proposed simple model for object replacement policies in cooperative caching system. The advantage of caching peer-to-peer traffic is to reduce the load on backbone links., The different view on the above topic, they had not focused on effectively traffic as well as on good performance for peer to peer proxy caching traffic.

2.3-Identify the APT malware Infections Based on Malicious DNS and traffic Analysis:

In the year of 2015, Gooding Zhao et.al had [11] purposed a novel system placed at the networks large point that aims to efficiently detect. APT malware infection based on the malicious Domain name system. The system uses the malicious DNS analysis technique to detect suspicious APT malware command and control domain and then analysis the traffic of the corresponding malicious IP using the signature-based and famously based detection technology. The author had also defined network traffic feature that can identified the traffic of compromised client that have remotely been controlling. This approach can not only reduce the volume of network traffic which need to be recorded and analysis, but also improve the sustainability of the system. The author had defined 14 APT malware server domain feature including dynamic DNS feature by studding large volume of DNS of traffic which can be called as big data. Abnormal network traffic feature is also defining to help to detect the traffic of compromised client that have been remotely controlled. They had built a particular device to decide whether an IP address is infected or not by using the feature of vector together. While comparing the botnet and worm, crafted APT malware required high -degree of stealth, for this reason the DNS behaviours feature of APT malware are un conscious These are hard to analysis large volume of inbound and outbound traffic is a large network, example- large enterprise and an ISP. The crafted APT malware attack do not used malicious flux service or DGA domain.

2.4. Defencing sychrophasor data network against traffic attack:

In the year of 2011, Biplab sika et.al had [12] present a set of approach to identifies the anonymity of sychrophasor data against passive traffic analysis attack, they purpose defence mechanism based packet concatenation and random packet drops as a counter measurement against attacks that may use different data information to compromise the network. The author has investigated susceptibility of the phasor measure unit data measurement and gathered network against a class of passive attack a develop a defence strategies against attack. The author focuses on the passive attack that are mainly concerned with privacy and anonymity issues. In passive attack, the attacker does nor resource but attempts to information from the system. The traffic analysis based on the passive attack aim to determine to identity and location of the communication hosts by observation the timing and length of message across the link in the network. They had present and evaluates a set of schemes, specifically tailored for sychrophasor measurement data, for defeating traffic analysis attack. The author has used an information theoretic measure to quality of the degree of anonymity provided by the proposed obfuscation strategies. They focused on the passive attack that mainly concerned with privacy and anonymity issue. The limitation is that; it is only focused on the traffic analysis attack. Doing the encryption process, it does not provide security to information, so that is exploited to the attacker.

2.5 Intrusion detection scheme using traffic forecast for wireless industrial networks:

In the year of 2012, Min Well et.al has [13] proposed an intrusion detection system for WIP-PN networks. After modelling and analysis traffic flow data by time sequence technique They introduce a new packet traffic model that is designed for intrusion detection in WIP-PN networks. They also assumed that the field device in WIP-PN network received become and send data based on super-frame cities. The wireless network for industrial automation process automation is a wireless network standard for industrial automation process automation. They have developed a unique requirement of industrial which use to satisfying anti-interference, low power consumption. The WIP-PN standard provided the mean to secure wired system. Intrusion detection system architecture the scheme has yet not been designed for wireless. The author develops new mechanism to protect the wireless networks wireless industrial network device provides limited resource in term of battery-power, low energy requirement, low processing, communication capacity etc. The industrial wireless network is based on event driven traffic generation, so that it cannot be used to detect the intrusion accurate. Industrial wireless network is not only designed for the specific requirement of industrial application but also for hid reliability and low energy consumption. The author provide scheme can effectively detect the intrusion attack, improve the network performance and for a long period of the network lifetime.

2.6 Benefits of traffic management for particular service IP network: for the learning different application:

In the year 2010, Chung Yu Choli has [14] developed the service management system that can analysis the traffic of individual service based on user log data. The author has developed a new traffic management system that can classified the individual service traffic link over the entire network and analysis user behaviour in the user of service with high economic benefit. STMS can report not only for the traffic of individual service in every link, but also user behaviour for each service. The unique feature of STMS that differentiates if from legacy traffic management system relying on passive measurement is the use of log data of individual service when STMS analysis the traffic volume of individual service in link. The STMS provide more accurately security and flexibility than the other networks During the verification of traffic computational of IPTV VOD service. The author also found that there is missing in the user log data are in the form of dispensable in computing service of traffic The author had found that their also missing in the traffic between the time of FF .They also found missing in term of while we turn off the STB the device it turn off automatically without alert any warning to the user .Another missing term in the STMS device is that the start time channel is present but end -time channel is not there for the user log data of IPTV channel service .In additional to service traffic ,they monitoring and management can expect the following metric for STMS as various area of application. The network designed can before more accurate because it can consider and area and service specific data easily reflect the change in traffic routes and network topology. The cost of individual service on network building and operate can be more accurately estimate. Knowledge of cases behaviour in the use of service in specific are in helpful when planning business and marketing strategy STMS is exported to offer a new way for network operating and new business strategy for global ISP facing the change network paradigm.

2.7. Post secrecy against traffic analysis attack in wireless sensor network:

In the year 2010, Xi Luo has [15] proposed three scheme to defence against the traffic analysis attack by random routing scheme is proposed to provide path identification. They combine random routing scheme with a dummy packet injection scheme to confuse the attacker by backtracking scheme from the packet. An anonymous communication scheme is proposed to hide the modified of all node that participate in packet transmission. Their scheme provides efficiently defend against traffic analysis attack, take less delivery time. The main contribution of these paper is 1) Rate-monitoring attack is based on the normal situation present near the node of base station forward a pattern of large amount of packets than the nodes. An attacker wants to captures the packet that used to send through nodes within its sensing range and move to the node which has a higher packet-sending rate. 2)Time interconnected attack also called packet tracing attack, an attacker captures the time between corresponding packets sending among nearest nodes and wants to trace it back the packet of each assist operation reaches the base station. The attacker may trace it back one packet lop- by-lop towards the base station.3) ID analysis aims at deduct the communication relationship between nodes and data traffic pattern through monitoring the identities of nodes which involved in the forwarded packet head. The author point of view their scheme, they use the amount of nodes remaining energy as the parameter to count probability that a candidate node will forward the dummy packet. Finally, they introduce an anonymous communication scheme to detect against ID analysis for the attacker by hiding all important information which ensures that the attacker can only collect a large pseudonyms pool but no relationship about the collect pseudonyms. The author these paper had some limitation, as they do not provide

protection to the encryption and authentication. The author introduces a novel random routing scheme for wireless sensor networks combined with dummy injection scheme based on relationship anonymous that defend against traffic analysis attacks in order to hide the locations of critical nodes. The author has proposed scheme can effectively prevent the traffic analysis attacks and has the less delivery time and energy consumption.

2.8 A Unique Approach to recognize P2P traffic based on program behaviours analysis:

Since year of 2011, Telexing Lihue's has [16] puts forward a traffic detecting mythology names peer detected which is based on the program behaviours analysis. The author has separate the traffic file sharing application from traditional application traffic and identify host which is participate in peer to peer activities. The peer to peer file sharing application have a unique connection pattern. They provide accuracy and efficiently to the peer to peer file sharing. They analysis the behaviours of file sharing applications for a huge number of connections to a lot of remote hosts. This feature helps us to identify the traffic of file sharing applications., Peer-Identifier is able to identified the large amount majority of peer to peer traffic effectively with a tiny probability of false positive and negative. Their evaluation is based on three scenes: pure scene, pure non-P2P scene and mixed scene. All the valid traffic is generated by the file sharing applications. The author mainly focuses on the explore similarly of inherent end -host in the same network prefixes and distant end-host behaviours cluster as well as application behaviours cluster. The benefit of the traffic pattern they used to identifies the attack in the form of anomalous and also detect the internet application behaviours through synthetic traffic.

2.9- Behaviour analysis of internet traffic via binary graph and one -mode projection:

In the year 2013, kuia Xu has present [17] a novel approach based on behaviours graph analysis to study the behaviour same to internet end host. They use bipartite graph to model host communication for the network traffic and built one-model projection of bipartite graph for discovery social behaviours same to the end-host. The author performed network aware clustering of end -host in the same network prefixes into the different end-host behaviour cluster and discover inherent clustered group of internet application. The author uses bipartite graph to model network traffic of internet backbone link internet facing link of border router in enterprise network. They subsequently construct one-model projection of bipartite graph to connect source host that communication with the same destination host connect destination host that communication with the same source host. They demonstrate practical benefit of exploring behaviours similarity of internet end-host in profile network prefixes and emerging application and detecting anonymity traffic pattern. The author studies the host behaviour at the social, functional and application level for classification traffic flow. While they build behaviour profile of end-host using traffic communication pattern. The author mainly focuses on the explore similarly of inherent end -host in the same network prefixes and distant end-host behaviours cluster as well as application behaviours cluster. The benefit of the traffic pattern they used to identifies the attack in the form of anomalous and also detect the internet application behaviours through synthetic traffic.

2.10 Noxious traffic analyses in wireless sensor network using advance signal processing technique:

In the year of 2013, Alexander Frankia [18] dais has proposed the encryption wireless transmission & detect the periodical component of the wireless traffic that can further reveal the a used in the sensor application. The author focuses on the study of traffic analysis that collect the timely patterns of the captured traffic. It reduces the power consumption required for traffic analysis. The author proposes countermeasures against malicious traffic analysis. The author has presented an attacker model that performs malicious traffic analysis in a WSNs. It consists of two:1) A malicious client overhears the wireless medium recording the timestamp of the capture packet.2) A malicious server using helps method is high and it successfully reveal the periodic component of the capture wireless traffic for high compression ratio

2.11 Fundamental of Vector and Network Traffic Analyse Detection:

In the year 2012, San chop Shin have [19] proposed two algorithms for network traffic monitoring and analysis, the author has proposed schemes are based on the data of a virtual vector that had recently invented, but limited to the purpose of estimating spread value. They found that the virtual vector that can be applied to a range of different problems in the area of network traffic. The author has proposed a counting virtual vector that counting the number of packets per-flow traffic measurement. For enlarge span flow detection, the author proposes a new detection scheme to catch even evasive flows. The author had cover three major topics in network traffic monitoring and analysis: spread estimation the per-flow traffic measurement. The spread of a source address is defined as the number of different destinations contacted by the source. They estimate the spread for each source. The author counts the number of packets per flow. All packets

belong to a particular flow have a set of common properties. The author has provided some properties are 5 packet header fields: source and destination IP addresses, source or destination port numbers, and these protocol type known as TCP 5 component. The author has proposed a new data structure, for per-flow traffic measurement. They proposed scheme that outperforms the state of the art scheme in measuring large flows and elephant. The author show that enlarge span traffic detection could easily be deluded by attackers.

2.12 DDOS identify algorithm based on pre-processing network traffic forecast:

In the year of 2013, Yuncheng Chen et.al [20] has proposed the pre-processing network traffic cumulatively average it with the time range by using the simple same AR model and then generating prediction network traffic. The author used a chaos theory to analyse it and proposed a novel network anomaly detect the abnormal traffic. The author also provide train a neural network to detect dynamic DOS attack. Distributing denial of service attack are launched by generating extremely large volume of traffic that rapidly exhausts a variable resource of target system to intentionally disrupt network service. It is difficult the compare the two dodos attack and normal attack specifically differential between dodo's attack from legitimate abrupt packet, so this make the dynamic DOS very damages to the network traffic. The time series method is being proposed by the author for modelling and prediction network traffic. The author has used a new pre-processing network traffic prediction method was proposed. The author has cumulative average network traffic with a time range which was with simple similar AR model to predict it and generate the prediction method for the network traffic. Author was proposed a detecting method against mimicking dynamic DOS attack has been proposed by using the chaotic analysis on new traffic network. The author has also use the chaotic analysis for predicting the error to detect the various distribution denial of service (DDOS) attack, which including mimicking distribution denial of service. Thus, by using these methods the author provided a burst tithe network traffic and also provide efficiency to the network traffic.

2.13 Deep cost indirect medium remote traffic attack in packet network:

Since year of 2010 Sachin Caldor [21] was provide a deep cost indirect traffic attack in packet based on network. The author used rate of sequence probes a remote attacker can be get the pattern traffic timing. The author also captures and monitor the policy is changed to round-robin that cooperative reduces significates the attacker can till reliable deduct user traffic pattern. The author has used to determine of need for considering an additional metric that instructed the information between the individual traffic flows through the router. The author uses attack against the traffic analysis that take advantage of the indirect flow that is introduce by should routing resource within network based packet. The author used to attack which can help to detect from attacker information and help him to protect them encrypt data such as account no and credit card. Monitoring at Scale. Author has successfully determined a nefarious attack that takes advantage of the indirect channel introduced by sharing routing resources within network based packet. The performance of the attack was shown using real traffic and simulation of first come and first server and round-robin policies.

2.14-Counter measurement of WIFI side channel analysis through traffic multiplexing:

In the year of 2014, Fan Zhang was [22] present was technique called traffic DE multiplexing which offers efficiency protection against wife traffic analysis without in critical noticeable overhead and performance degradation. The author had approach utilize media access control layer virtualization a packet scheduled over multiple virtual MAC to shape the traffic on each virtual MAC interface. Traffic multiplexing operate at the MAC layer analysis transparent to user and other protocol stack. They implement their technique over multi-hop Author, Drive for Wi-Fi and evaluate it the real WLAN environment. The author demonstrates that traffic de-multiplexing in efficient in defending against traffic analysis attack and easy to develop. Threat of traffic analysis is particular evil in wireless network, which has been widely develop in residential, hotspot and campus environment for the internet access. Due to these shared medium nature of wireless link the attacker can easily attack on the specific user traffic using sniffer software. To achieve both efficiency defence against traffic analysis the author present a novel design called traffic DE multiplexing. The author has been developing an idea is to petition a Wi-Fi traffic flow into when transmitting these packet through different virtual media access control interface of Wi-Fi channel. To improve the performance of traffic DE multiplexing the author has used strategies 1) They will have disabled the ACK frames in this paper. But disabled ACK may incur the unreliable transmission and then a significant loss of throughput in a large WLAN. 2) The parameters of virtual interfaces and DE multiplexing scheduling policies of APs and clients are able to change adaptively and dynamically according to the transformation of Wi-Fi networks. 3) The author will perform traffic DE multiplexing and validate its performance for a wide range of practical network scenarios in future work.

2.15-Encounter algorithmically generated domain-flux attack with DNS traffic analysis:

In the year of 2012, Sandeep Yadav [23] was develop a methodology to detect such "domain –flux in DNS traffic by looking for patterns inherent to domain names. The author present and compare the performance of several distance metrics, including Edit distance, and Jacquard measure. The author has train by using a good dataset of domains obtained via a crawl of domains mapped to all IPv4 address space and modelling bad datasets based on behaviours of the data. The author also apply methodology to packet traces collected at a Tier-2 ISP. They can automatically detect domain fluxing as used by Conifer botnet with minimal false positives, in addition to identify a new botnet within the ISP trace. Author also analyses a campus DNS trace to find another unknown botnet exhibiting advance domain name generation technique. The author develops metrics different technique from the signal to detect theory and statistical learning that can detect algorithm generated domain names that may be generated via a myriad of techniques. The author has proposed a theoretical analysis on DNS traffic to identify of and when the domain name is being generated by algorithm to give protection against other attacker and, they have used technique as amorously detection to provide against the DNS queries and domain name flux. So that the author proposed a theoretical analysis on the present bot with network and network administration can disconnect the bot from that attacker command and control server by filtering DNS queries.

3. CONCLUSION

Since last 10 years the network traffic analysis has increase massively over the last couple of years Several modes were proposed throughout the years to address existing scientifically issues. Traffic analysis tasks may be supported by hard - work computer software programs. Advanced traffic analysis techniques may include various forms of social network analysis Traffic flow security is the use of measures that conceal the presence and properties of valid messages on a network to prevent traffic analysis. The traffic analysis can perform med in the context counter measurement, IDS, industrial networks. WSNs.To protect from different malicious attack in my survey paper I had mention intrusion detection system which will protect form different malicious attack and attacker. This survey paper summary on the traffic analysis, IDS, traffic analysis related to the WSNs, different type of attack in internet traffic analysis, traffic analysis measurement etc. In the above paper 9 on that they were discuss on the clustering algorithm they have analysis different pattern of IP prefixes and detect anomalous traffic behaviour, so I can extend these clustering algorithm in my future work. Same as the 2.11 on that, they had used two algorithm per-flow traffic measurement and another to detect the long –duration of the traffic flow, so I can use and improve their algorithm in my future work for providing protection and improve efficacy to my system. In the case of the 2.1, on this paper they have discussion on the analysis of false positive and false negative from real traffic analysis with intrusion detection system and prevention system, the author uses the FPNA mechanism in the libpacp system to provide contexture analysis of false positive cases. FPNA collected more than three thousand of False negative and False positive. The FPNA mechanism consist of three components as majority voting, trace checking and traffic analysis.by using these mechanisms they can verifies the different technique. They use IDS and IPS to provide reliability.so I can apply these techniques in my future work. In the case of 2.4 article they have discussed on the protection of the enormity of synchro phasor data against passive traffic attacks, they have used two algorithms: packet concentration and random packet drop as a counter measure against the different traffic attack in networks. They have used mix technology. So I, can used these mix technologies in my packet routing doing my future The working of mix technology on the basic of public key cryptography, so I can improve these technique and use these in my future work. These survey will definitely create interest among the student those are want to research on the traffic analysis.

S.NO	YEAR	PROPOSED WORK	ADVANTAGE	DISADVANTAGE
1	2012	Data analysis of FN and FP in real traffic analysis in IDS/IPS	1- IDS produce relative alert and passes it to network administration promptly while the IPS not only execute what the ids does, but also identifies the malicious source. 2- The FN and FP both are used in IDS and IPS which provide efficiency to network system.	1-The signature based detection are missing in the both of cases in the FN as well as the FP. 2-The false positive and false negative provide less reliable to the IDS/IPS detecting system.
2	2010	Deep-cost indirect medium remote traffic attack in packet networks	1-They improved the performance by using FCFS and Round-Rabin algorithm in the real time.	1-The author have not used articherture of internet launching such that the attack is infeasible because it would acquire high bandwidth and time.

3	2010	On the assert of cooperative proxy caching for peer-to-peer traffic.	1-The advantage of caching peer to peer traffic is to reduce the load on backbone links. 2-They also reduce the cooperative cost of ISP	1-They had not focused on effectively traffic as well as on good performance for proxy caching traffic.
4	2015	Identify the APT malware infection based on malicious DNS in traffic analysis	1- They focused on the passive attack that mainly concerned with privacy and enormous attack.	1-They have only focused on the traffic analysis attack.
5	2012	Fundamental of vector and network traffic analysis Detection	1-The author use counting virtual vector that counts the number of packets for per-flow traffic measurement,	1-The long -duration flow in not heavy so that the attacker scan easily their data.
6	2013	Malicious traffic analyses in wireless sensor network using advance signal processing technique	1-They are easily developing in large and harsh area. 2-They used the traffic analysis method for energy consume and improve efficiency. Also improve the probability of extract signal while Gaussian distribution	1-The advantage of these article is the extract signal is very high proclivity, while using Gaussian distribution.
7	2013	DDOS identify algorithm based on pre-processing network traffic prediction.	1-By the used of DDOS mimicking method they improve the efficiency of the network and also provide burst to the network	1-DDOS miming is difficult to detect in real time and normal attack.
8	2011	Defencing sychrophasor data network against traffic attack.	1-They focused on the passive attack that mainly concerned with privacy and anonymity issue.	1-They only focused on the traffic analysis attack. Doing the encryption process, it does not provide security to information, so that is exploited to the attacker.
9	2013	Behaviour analysis of internet traffic via bipartite graph and one -mode projection	1-By the used of cluster algorithm they provide defence against anonymous system. 2- The article focus on the individual accuracy prefix data	1-AS the recent research different author focused on the web service such as HTTP, DNS etc.
10	2012	Intrusion detection scheme using traffic predication for wireless industrial network	1-Wireless industrial network prove ide high reliability and low-energy consumption. 2- Wireless industrial network provide effective detection against attacker to improve the overall network and prolong the network life.	1-Wireless industrial network provide limited battery-power, low-energy requirement. 2-It does not provide accurate detection to industrial propose.
11	2014	Thwarting wife side -medium through traffic DE multiplexing	1-By the used of WLAN testbed and sniffing technology they provide effectiveness and efficiency to traffic DE multiplexing against different attacker. 2- They also provide good scalability and suitability for WLAN development in hotspot.	1-They have ignored the communication layer for DE multiplexing.
12	2010	Benefits of traffic management for different service IP network: Learning for different application	1-The STMS provide unique feature for traffic management system relying on passive management which used for logging data for the individual service. 2-STMS provide accuracy and flexibility to the network.	1-Duing the verification of IPTV VOD, the user log data is missing. 2-IPTV the end -time channel for user is missing.

13	2010	Post secrecy against traffic analysis attack in WSNs.	1-They provide efficiency defence against attack and take less delivery time. 2- They protect against different attack by using different type of attack such as rate-monitoring attack, time correlated attack, ID analysis attack.	1-The main disadvantage of these article it does not provide protection to the encryption and authentication.
14	2011	A unique approach to recognize P2P traffic based on program behaviour analysis	1-This article provide a unique file sharing pattern. 2-It provide efficiency in accuracy to file sharing.	1-It is difficult to detect the P2P traffic. 2-It provide poor quality of network service.
15	2012	Encounter algorithmically generated domain-flux attack with DNS traffic analysis	1-The author has used large dataset to improve the performance of the Domain 2- The author have use TLD (top level domain), the Edit distance by the use these, they have achieved 100% detection and 10% false positive.	1-In the previous paper, the author has identified the inner-working in IP flux fast network for hiding spam and san infrastructure.

REFFERNECES

[1] Introducing Traffic Analysis, George Danezis and Richard Clayton, January 21, 2007

[2] A survey on internet traffic identification Arthur Callao, Carlos Kaminski Member, IEEE, Gaza Szabo, Balassa Peter Giro, Judith Keller, Steno Fernandez Member, IEEE, and Jamel Sadoski, Senior Member, IEEE

[3] Toward an analysis approach to anonymous wireless network, par venkitasubramaniam, ting he Lang and Stephan B. wicker, Cornell university IEEE communication magazine 2008

[4] TCP Throughput Enhancement over Wireless Mesh Networks, Li-Ping Tung and Wei-Kuan Shih, National Tsing Hua University The-Chung Cho and Yeali S. Sun, National Taiwan University Meng Chang Chen, Academia Sinica, IEEE Communications Magazine • November 2007 IEEE

[5] G. Barrenetxea, F. Interest, G. Schaefer, M. Petteril, O. Coach, and M. Parlance, "Sensor Scope: Out-of-the-Box Environmental Monitoring," in Proc. of IPSN, 2008.

[6] A. Milinkovic, C. Otto, and E. Jovani, "Wireless sensor networks for personal health monitoring: issues and an implementation," Computer Communications, vol. 29, pp. 2521–2533, 2006

[7] Intrusion detection system based on traffic analysis in wireless sensor network, Ponomarochuk, yulai and see, Dae-Wha Dept. of Electrical Engineering and Computer science kyungpook National University Daegu www. wileyindia.com - Principal of Computer security, by Bible.

[8] Statistical Analysis of false positive and false Negative from real traffic with intrusion detection/prevention system, Cheng-yuan conational Chiai Tung university Yuan-change Lai, National Taiwan University of science and technology iwi chai, fury Wang and wei-hsuna tai, national chain Tung university. IEEE 2011

[9] On the benefits of cooperative proxy caching for peer-to-peer traffic Mohamed hafted senior member, IEEE and Behrouz Noorizadeh vole 21 no 7 July 2010

[10] Detecting APT Malware infection based on malicious DNS and traffic analysis GUODONG ZHAO, KE XU, (senior member, IEEE) LEI XU, AND BO WU, IEEE July 20 2015

[11] Defending Synchro phasor data networks against traffic analysis attack, Byplay Sirdar, senior member, IEEE and Joe H chow, fellow, IEEE VOL2 NO 4 December 2011.

[12] Intrusion detection scheme using traffic prediction for wireless sensor network, Min Wei and Beechen Kim vole 14, no 3 July 2012.KICS

[13] Service traffic management system for multiservice IP network: Lessons Learned and Applications Zing Yue choir, sung kwacha, Mah-jong lime, teal chase, young-kwon shim and jae-hyoung you.

[14] Location Privacy against Traffic Attacks in Wireless Sensor Networks, Xi Luo, Xu Ji, Muong-Soon Park∗ Department of Computer Science and Engineering Korea University, Seoul, Korea {Rosa-xi, jinx, myongsp} @ilab.korea.ac.kr), IEEE 2010.

[15] A Novel Approach to Detect P2P Traffic Based on Program Behaviour Analysis, Telexing Liu State Key Laboratory of Networking and Switching Beijing University of Posts and Telecommunications Beijing,

[16] behaviour analysis of internet traffic via bipartite graph and one -mode projection, Kuia Xu Member, IEEE, ACM Feng Wang Member, IEEE and Lin GU Member, IEEE vole 22 NO 3

[17] Malicious traffic analysis in wireless sensor networks using advanced signal processing techniques Alexandros Fragkiadakis, Iohannis Askoxylakis Institute of Computer Science Foundation for Research and Technology-Hellas.

[18] Virtual VECTOR and Network Traffic Analysis, seon-Ho and MyungKeun Yoon, kombi University.

[19] DDOS Detection algorithm based on pre-processing network traffic prediction.

[20] Low-Cost Side Channel Remote Traffic Analysis Attack in Packet Networks, Sachin Caldor†, Xin Gong†, Negar Kiyavash‡, Toga Tuscan§, Nikita Brasov† † ECE Department and Coordinated Science Lab.

[21] Thwarting Wi-Fi Side-Channel Analysis through Traffic DE multiplexing, Fan Zhang, WeMo He, Yangzi Chen, Zhou Li, Xiao Feng Wang, Shoo Chen, and Xu Liu, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 13, NO. 1, JANUARY 2014.

[22] Detecting Algorithmically Generated Domain-Flux Attacks with DNS Traffic Analysis, Sandeep Yadav, Student Member, IEEE, Swath Kumar Krishna Reddy, A. L. Narasimha Reddy, Fellow, IEEE, Member, ACM, and Supranamaya Raman, Member, IEEEACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 5, OCTOBER 2012

AUTHOR BIOGRAPHY

Saurav Mishra had received the bachelor of Technology at Gandhi Engineering college, khudra Bhubaneswar India. Currently pursing Master Degree in KIIT University Bhubaneswar, India. Currently doing Research work on Traffic Analysis, Networking.

Manjusha Pandey had received bachelor degree at Indian Institute of Information Technology, Allahabad (IIIT). She has done Master degree from Indian institute of information Technology, Allahabad in 2010 India.She is working at Allahabad and KIIT University, Bhubaneswar, India. She has done Research on the wireless sensor network, privacy and security, HCI.

Gargi Srivastava had received bachelor degree at Shri Ram murti Smarak college of Engineering and Technology, Breilly.She is currently working at KIIT University as Assisient Proffession.She has done Research on traffic analysis, energy conservation, Networking,