A New Local Area Network Attack through IP Address Spoofing

S.N.Sheela Evangelin Prasad[1] & Dr. M.V.Srinath[2]
[1]Research Scholar,Department of Computer and information Technology,Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli 627 012, Tamil Nadu, India.
[2]Director, Department of M.C.A, STET Women's College, Mannargudi, Tamil Nadu, India.

Received: September 02, 2018 Accepted: October 22, 2018

ABSTRACT *One of the major challenges in the computer networking is avoidance of intruder whereas several data's are confidential and personal in all the areas like organization, banks, financial sectors, health care etc. In order to avoid the intruder, all the activities should be logged into an Intrusion Detection System(IDS) for identifying any malicious activity which is being performed on the network system. The normal scenario if the attacker wants to download the file without proper authorization can be done through copying the URL and download the file easily.In computer networking, IP Spoofing with false source IP address is the creation of Internet Protocol(IP)packets for the purpose of impersonating another computing system or hiding the identity of the sender. This paper proposes security for protecting the network from the attacker using IP Spoofing technique.According to the cryptography mechanism the authorized user can able to download the encrypted datawhich can be decrypted usingDES andsecret key mechanism using random key generation for secure transmission of data in LAN Network.The performance evaluation of data transmission speed is compared with IP spoofing and without IP spoofing.*

Keywords: *IP Spoofing, Network,secret key, encryption,attacker*

1. Introduction

In this period the explosive growth of internet gets added through new services in the developing network which has also included security attack impacts. In order to protect the network from all intrusion these services are implemented through software application and operating system namely antivirus, antispam, firewall etc. Today's network organization, security is the important features in network technology of each network infrastructure is quickly increasing internet for most of the organizations. Because of this many of the problems have been faced to secure energetic resources and vital information in the network Mehdi Bahrami,et al(2011)[1]. Interruption is an act of accessing and utilizing the data in computer properties without freedoms, thus initiating attendant security and damage breach. In this network, the process of exploring and detecting events can occur in the computer is said to be intrusion detection which has to identify security openings, i.e. the development of identifying the actions with interfering behavior. Intrusion Detection System (IDS) examines the traffic of network and classifies the activities that interrupts the security based on policy of computer network which provide a warning signal or message about the threat to the network or system has been detected. IDS analyze based on all security threats the operations of firewall, routers, servers,critical files for intrusions and conveys a defensive model for which causes damage to the network and also identify the attack that related to traffic in network is made to be the attack that related to traffic in network is made to be blocked. One of the complex models is network control whereas the IDS implementation has created a network delay. Therefore, advancement in various software based network related with IDS are available. Thus the model has a problematic with the traffic of high speed Sheela,et al(2015)[2]. Though the IDS major objective is for detecting intrusions, it also certain to deliver the following services:

- Audit the scheme structure and susceptibilities.
- Evaluation of network reliability, hardware and archives.
- Tracking irregularities.
- Perceiving and examining system for network activities.
- User friendly border are providing to security management.

The significant and beneficial data is often interested from attacker which is constantly accountable for most of the attacks through networks. Attacks are done in the network server or system from the attacker by sending malicious packet into the user network for privacy, damaging or altering unrevealed data or significant data. These kind of activities is done by network packet sending through network to the purpose of illegal is said to be attack. This attack may occur through network server or system because of vulnerability or any current weak system namely system misconfiguration, program error and user misuse. An astute attacker may also be created using multiple of vulnerabilities as collectively. In this global network, there are enormous large size server and wide number of online service organized in the network.

Hence, most of the attacker get attracted to this network and required rational intrusion detection model as a defense to its network system Aanchal kumar,et al(2016)[3]. IP spoofing represent as the internet protocol (IP) packets has created in the network with a fake source IP address whereas the resolution of disguising sender distinctiveness or portraying other computing networks. In this spoofing attack, the attacker has send a message for indicating the user with the message which is received from a trusted system IP address and packet header modification is done that packets seem to be send from the trusted system. The major significance of the attacker is spoofing the destination end computer to believe that sender is authentic person of the network. Hence, the focus of this attack is for creating a link which permits the attacker to benefit the root access from the host. This entry is a creation of bypass path entry to achieve the target system. Nowadays, several equipment of the network has transmitted data in a plaintext at the layer of data link that has exposed significant data namely IP address, protocols of the application and port number to an attacker which easily create a path for attacking network. This research work proposes a IP Spoofing technique for securing the network from the intruder and also assures its safety. This technique is used to detect common attacks LAN network systems. The detecting mechanism of IP spoofing will initially identify whether the packet is malicious or not. Once the malicious is found then it tries to recognize the origination of the true source IP packets. The IP address matching (IP spoofing) is encountered to verify the user authorization and it reveal the file sets at the server. The secret key is encrypted the file using random key generation for secure transmission of data viewed by the authorized user in LAN Network. The performance evaluation data transmission speed is compared with IP spoofing and without IP spoofing.

2. Literature Review

The set of activity has endeavor for compromising the resource confidentiality, integrity and availability whereas IDS has determined the action of illegal that performed from computer system and also modify the administrator system. This paper has proposed intrusion detection mechanism of database for enhancing the database security over a website Yashashree,etal.(2017)[4]. The researcher has contributed a goal in taxonomy, current dataset configuration survey and current IDS assets and capability. To improve the efficiency of IDS, the next generation IDS to build the creation of datasets and also for network threats reflection with high accuracy in the future datasets Hanan Hindy,et al.(2018)[5]. This detection of framework with irregularity threats and an unreliable fluctuation in its properties and traffic qualities has considered some necessary activities whereas raising an alert message is the best example. There are several recent NIDS framework in this manuscript gets used for battling the security threat and recognizing Ankit punia,et al.(2017)[6]. This paper described to defend our data uses the technique based on encryption for data security. Encryption process is very simple technique for entire security of data that even can't able to legible using their server which have secured the calls and the messages at highest possible security Rupali Gharde,et al.(2017)[7].This study has deal with various algorithm or technique utilized to secure the data in public cloud Gowthami,et al.(2017)[8]. In this research work, different kind of network security get focused on reviewing the concept of cryptographic and discussing about the cryptographic algorithm range and other mechanism of security which are endorsed for preventing any attack namely destroying, modifying, exposing, stealing of data and benefit in unauthorized access to the system over network Tanveer(2017)[9]. The study about transmission of confidential message securely from one end to other end is called cryptography and it plays an essential role for securing confidentiality of data while transferring data particularly via Internet.There are few security requirements namely authentication,integrity,confidentiality and non-repudiation within the context of any application to application Dongare,et al.(2017)[10].This paper discuss about the novel behavior of detecting architecture which utilized the same measurement for detecting and also activities of insider Robertkoch,et al.(2015)[11]. This present a entire study of detecting intrusion, various type in intrusion detection, several kind of attacks, various technique and tools, required research, challenges and at last developing the IDS tools that are able for detecting and preventing the intrusion from the intruder Mohit Tiwari,et al.(2017)[12]. The mimic encryption system is proposed in this paper for protecting a network from attack and also assures their security as the network security Bin,et al.(2018)[13]. This paper to makes it secures that an alteration to the Data Encryption Standard(DES) and immune to errors which are caused by the wireless channel.When the modification algorithm is used in the wireless channel has improved the performance of bit error rate and also the security compared with DES Zibideh(2015)[14]. The growth of network technology any type of information can easy to send and receive. The process of cryptography mechanism is not understandable by intruders or unauthorized users based on different algorithms Maninder Kaur,et al.(2017)[15].During past decade years, there are several cryptographic algorithm have advanced but each user is in need of cryptographic algorithm that accomplish

a best level of security and performance. According to the cost performance, there are various algorithm get trade off but user may choose any of the cryptographic algorithm based on their needs Sandip Thitme,et al.(2016)[16]. The DES is cryptographic algorithm based on block cipher technique which is applied with a data block concurrently instead of a bit at a time Bhawana Singh,et al.(2016)[17]. This proposes a SVT to defend from IP spoofing attacks whereas this method has validates IP address of each Autonomous System (AS) and Neighbor Authentication (NA) algorithm Alwar Rengarajan,et al.(2016)[18]. This paper describes the detection and prevention methods on communication system by IP spoofing Sharmin Rashid,et al.(2013)[19].This study has illustrated the damage in communication system due to IP spoofing whereas this mechanism has provided a shield against IP spoofing using the concept of cryptography key exchange algorithm and this result is discussed through NS2 as simulations Abhishek and Manoj(2013)[20].

3. Methodology

In this network, proposed security technique is used at both end namely source or sender and destination or receiver. In the source end, files or data which need to be transmitted are uploaded with encrypting the data using Data Encryption Standard algorithm(DES)and then secret key is used for authentication.Afterthis encryption is completed, view all the IP address from the LANand stored in binary files whereas most of them are numeric data files with the extension of 'arp' format. Moreover, extraction of all the IP address from the bat files is known as IP Extraction. This is made in the progress of line by line and stored in array object for clearing the noise in preprocessing method. Once this process gets completed,sender selects the receiver destination in the network by hiding the IP address and the port number with inclusive of the encrypted data to destination end. In the destination end,checking of buffer IP addresswith receiver end system configurationby checking it using the hidden IP address and the port numberof the destination end.Once it gets matched the receiver IP and buffer IP the authentication verification is done by giving the exact secret key in the network.IP spoofing specification is shown in figure.1.This proposed model is illustrated in the two phase namely,

1. Sender End Phase
2. Receiver End Phase

3.1 Sender End Phase

In this phase, data's which is to be uploaded are encrypted using DES algorithm whereas this kind of encoding is done to avoid unauthorized person for viewing the context of the data and only the authorized person can able to view through secret key which is provided from the corresponding sender is shown in figure.2.In this intra-network, all the IP address have unique set of numbers which are separated using the full stops are used foridentifying each computer using IP to communicate over a network whereas this gets stored in binary file format (.arp). Hence, the IP extraction is done by extracting line by line with all the IP address in the LAN network and stored in array object in order to remove noise by preprocessing method. A sender accesses intranet from their local computer which has IP address 192.168.0.5 and selects the receiver IP address 192.168.0.6 in the network, this receiver IP address and port number is hidden and the sender sends the encrypted data to the destination IP address 192.168.0.6 which is authorized IP address.

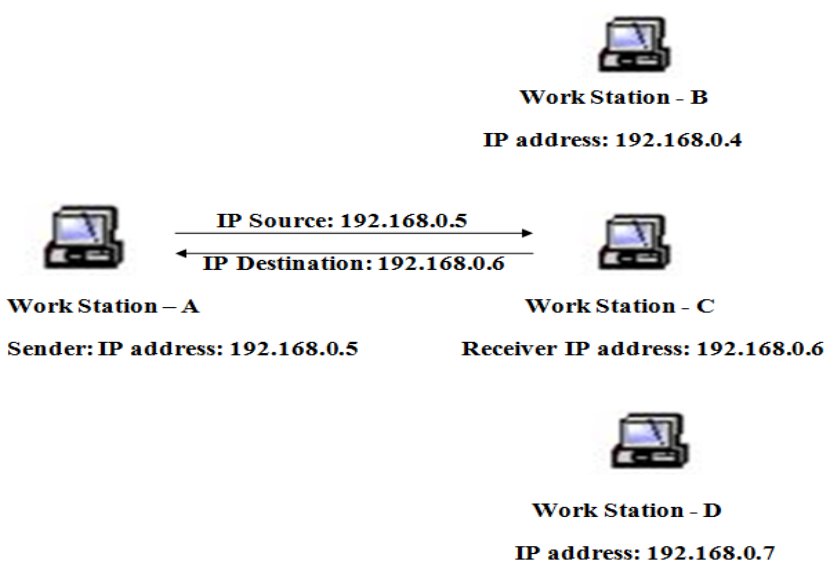

Figure.1 IP Spoofing Specification

Pseudo Codes

1. IP Extraction

Process builder (bat file path)
Start.process
While (true)
Readline by line
If (Match with pattern)
While (if pattern matched means)
Extract ip by ip digits
Close reader
Split ip based on index value
Get Host Name from IP

2.NOISE Removal

String var = bat value text
Var convert to arrays[]
Split array[] line by line
Remove after (192.168.1. with 2 digit) text
Store only ip address

3. Hide IP Address

Read text file from user chosen file path
Bufferedreader
While (read line by line)
String temp var
Temp+=Store all texts
Merge with ip,port,four keys,receiver info
Temp+=receiver info (IP PORT)
Send text by bufferedinputstream
With socket byteArrays

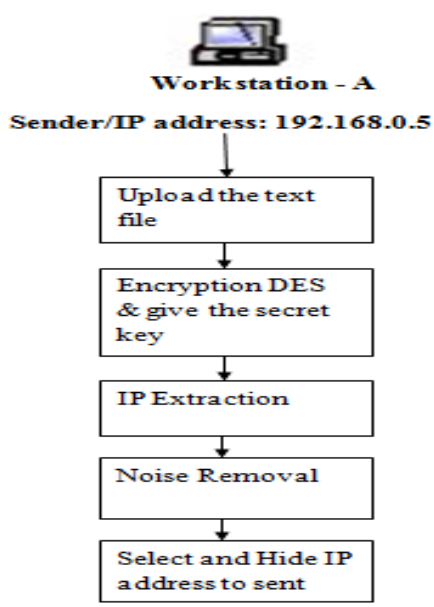

Figure.2 Sender End Phase

3.2 Receiver End Phase

In this phase, the source data is received in the destination end. The receivers IP address 192.168.0.6 checking the buffer IP address. In the destination end is shown in figure.3 checking of buffer IP addresswith receiver end system configurationby checking it using the hidden IP address and the port numberof the

destination end. If it is matched the receiver IP and buffer IP the authentication verification is done by giving the exact secret key in the network. In order to confirm whether the destination receiver is an authenticated person to view the data, the respective receiver has to provide the IP address and port number in order to receive the data.

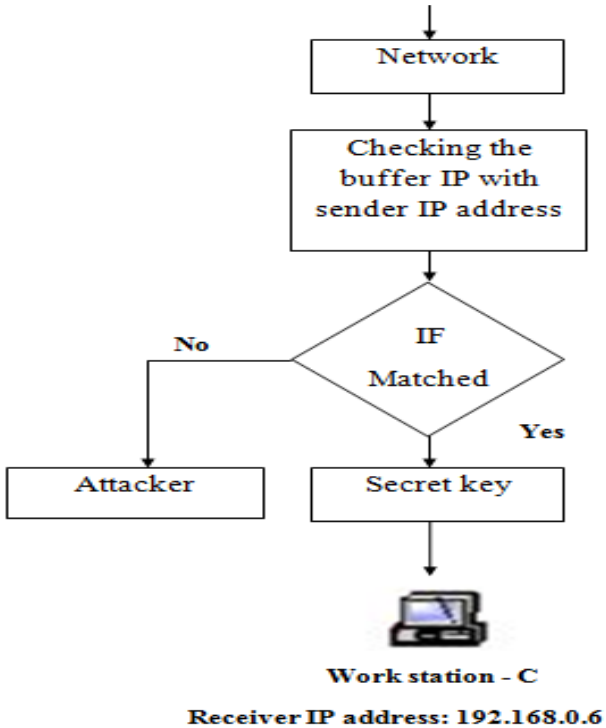

Figure.3 Destination end phase

4. Performance comparison

In this work the data transmission speed is compared with IP spoofing and without IP spoofing. The data are send by IP spoofing has higher speed than the data send without IP spoofing. Comparison graph for bandwidth level with IP Spoofing and without IP Spoofing is as shown in figure.4.

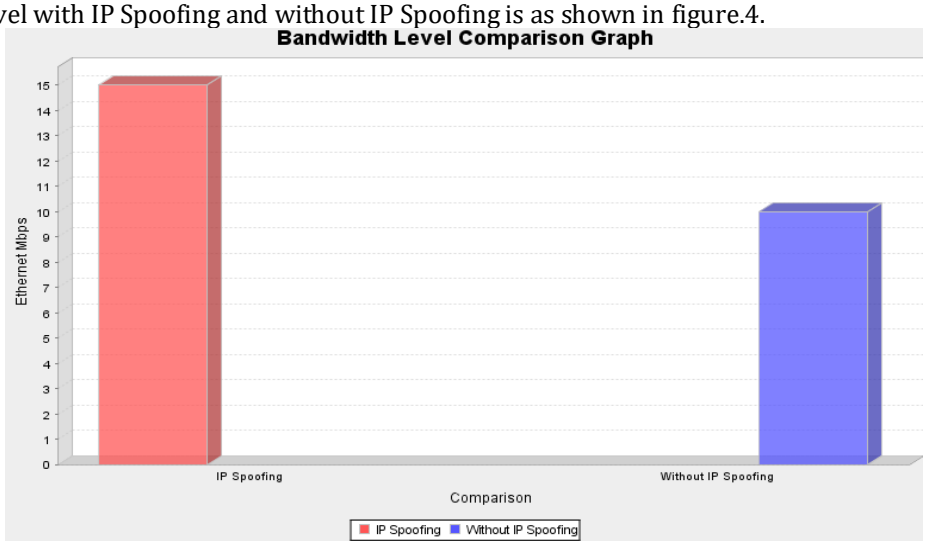

Figure.4 Comparison of Bandwidth level

5.Conclusion

The proposed IP spoofing technique has focused on securing the data while transmitting from one system to another system in the computer network. The IP address spoofing is encountered to verify the authorized user and reveal the file sets at the server. The unauthorized user will try to receive data using IP address in destination end, checking of buffer IP address with receiver end system configuration by checking it using the hidden IP address and the port number of the destination end. Once it gets matched the receiver IP and

buffer IP the authentication verification is done by giving the exact secret key in the network otherwise intruder IP address is send to the source end as an error message.The performance evaluation of the bandwidth level with IP Spoofing is higher speed which is illustrated that has better robustness and secure transmission of data in LAN Network.

REFERENCES

1. Mehdi Bahrami and Mohammad Bahrami , "An overview to Software Architecture in Intrusion Detection System", 2011,International Journal of Soft Computing And Software Engineering (JSCSE),ISSN: 2251-7545 Vol.1,No.1, 2011.
2. S. N. Sheela Evangelin Prasad, M. V. Srinath and MurtazaSaadiqueBasha , "Intrusion Detection Systems, Tools and Techniques – An Overview" , December 2015,Indian Journal of Science and Technology, Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/80108.
3. Er.Aanchal Kumar, Er.JaspreetKaur andEr. Inderpreet Kaur, "Intrusion Detection System by Machine Learning Review", 2016, IJARIIT,ISSN: 2454-132X, Volume2, Issue3.
4. YashashreeDawle, ManasiNaik,SumedhaVande and Nikita Zarkar , "Database Security Using Intrusion Detection System" ,2017, (IJLERA) ISSN: 2455-7137,Volume – 02, Issue – 03, PP – 01-06.
5. HananHindy et.al, "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets" , 2018,Association for Computing Machinery, Vol. 1, No. 1.
6. Ankit Punia and VedangRatanVatsa, "Current Trends and Approaches of Network Intrusion Detection System" , IJCSMC, Vol. 6, Issue. 6, June 2017, pg.266 – 270.
7. RupaliGharde and Archana Augustine, "Anomaly Detection with Cryptographic Operations and Transient secrets in CipherXray" ,2017,International Journal of Innovative Research in Computer and Communication Engineering,Vol. 5, Issue 3.
8. R.GowthamiSaranyaand A.Kousalya, "A Comparative Analysis of Security Algorithms Using Cryptographic Techniques in Cloud Computing" ,International Journal of Computer Science and Information Technologies, Vol. 8 (2) , 2017, 306-310.
9. Mohammad Tanveer Khan, "Review: Network Security Mechanisms and Cryptography" ,July 2017, IJCSMC, Vol. 6, Issue. 7,pg.138 – 146.
10. Ashish S. Dongare, Dr. A. S. Alvi and Prof. N. M. Tarbani, "An Efficient Technique for Image Encryption and Decryption for Secured Multimedia Application" , 2017,IRJET, Volume: 04 Issue: 04.
11. Robert Koch et.al, "Behavior-based Intrusion Detection in Encrypted Environments",15 July 2015,IEEE Communications Magazine, Network & Service Management Series, VOL. 11, NO. 4.
12. MrMohit Tiwari, Raj Kumar, Akash Bharti and Jai Kishan, "Intrusion Detection System" ,International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com, Volume 5, Issue 2 (March - April 2017), PP. 38-44.
13. Bin Li ,Qinglei Zhou, Xueming Si and And Jinhua Fu, "Mimic Encryption System for Network Security" , 2018, IEEE. Translations and content mining are permitted for academic research only, Vol 6.
14. Walid Y. Zibideh and Mustafa M. Matalgah, "Modified data encryption standard encryption algorithm with improved error performance and enhanced security in wireless fading channels" ,2015,Security and Communication Networks.
15. ManinderKaur ,Navpreet Kaur and Baldeep Singh, "Comparative Study Of Different Cryptoghraphic Algorithms" ,May 2017, International Journal of Advanced Research in Computer Science ,Volume 8, No. 4.
16. SandipThitmeand Vijay Kumar Verma, "A Recent Study of Various Encryption and Decryption Techniques" , International Research Journal of Advanced Engineering and Science, Volume 1, Issue 3, pp. 92-94, 2016.
17. Bhawana Singh, Rishi Sharma, Kamal Kant Verma and Satendar Kumar, "Enhanced key-generation algorithm using MRMCTT in Data encryption standard algorithm",International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 5, Issue 5, May 2016.
18. AlwarRengarajan, RajendranSugumar andChinnappan Jayakumar, "Secure Verification Technique for Defending IP Spoofing Attacks" , The International Arab Journal of Information Technology VOL. 13, NO. 2, March 2016.
19. Sharmin Rashid and SubhraProsun Paul, "Proposed Methods of IP Spoofing Detection & Prevention" ,International Journal of Science and Research (IJSR),Volume 2 Issue 8, August 2013.
20. Abhishek Kumar Bharti andManoj Chaudhary, "Detection of Session Hijacking and IP Spoofing Using Sensor Nodes and Cryptography" ,IOSR Journal of Computer Engineering (IOSR-JCE), Volume 13, Issue 2 (Jul. - Aug. 2013), PP 66-73.