IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DEMONSTRATE THE PERFORMANCE OF AN PASSIVE IP TRACEBACK MECHANISM OVER SPOOFED NETWORK

MUCHAKARLA VENKATA RAO [#1], A. DURGA DEVI [#2]

[#1] MSC Student, Master of Computer Science,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

Abstract

In current days there were a great deal of assaults that happen in the field of software engineering and data innovation during the procedure of information transmission from one area to other area. In spite of the fact that the information will be moved from one area to other with a substantial IPaddress and port number inside the system, there is an opportunity of happening assault during information transmission in any capacity. One among the few assaults is IP-Spoofing assault which goes under a few assaults that are accessible in writing. This IP-Spoofing assault comes in various manners dependent on their assault type. The procedure or strategy for making a web convention (IP) parcels with a phony IP-Address or obscure IP address and attempt to sends to another framework with an off-base or phony ID ipaddress is known as IP-Spoofing. In this proposed application we attempt to configuration PIT model known as Passive IP Trackback model in which if there is any Spoofing assault is discovered it will quickly backtraverse for one hub back to its past root and attempt to send the information to legitimate goal with the assistance of other moderate hubs. By directing different analyses on our proposed PIT model, we at last arrived at a resolution that our proposed model is effective in catching the area of IPSpoofers dependent on way backscatter informational index and as an expansion we have indicated the application under a recreation graph with hubs and their assault situation is recognized effectively through that diagram model.

Keywords : Ipaddress. PIT Model, Backtraverse, Ipspoofers

1. INTRODUCTION

IP SPOOFING, which implies aggressors propelling assaults with manufactured source IP addresses, has been perceived as a genuine security issue on the Internet for long . By utilizing addresses that are doled out to other people or not alloted by any means, aggressors can abstain from uncovering their genuine areas, or upgrade the impact of assaulting, or dispatch reflection based assaults. Various infamous assaults depend on IP mocking, including SYN flooding, SMURF, DNS intensification and so on.

A DNS intensification assault which seriously debased the administration of a Top Level Domain (TLD) name worker is accounted for in this framework. In spite of the fact that there has been a well known standard way of thinking that DoS assaults are propelled from botnets and satirizing is not, at this point basic, the report of ARBOR on NANOG 50th gathering shows caricaturing is as yet noteworthy in watched DoS assaults. To be sure, founded on the caught backscatter messages from UCSD Network Telescopes, ridiculing exercises are still much of the time watched .

In any case, to catch the starting points of IP caricaturing traffic on the Internet is prickly. The examination of distinguishing the starting point of mocking traffic is sorted in IP traceback. To fabricate an IP traceback framework on the Internet faces at any rate two basic difficulties. The first is the expense to receive a traceback component in the steering framework. Existing traceback systems are either not broadly bolstered by current product switches (parcel stamping), or will acquaint significant overhead with the switches (Internet Control Message Protocol (ICMP) age , bundle logging), particularly in superior systems. The subsequent one is the trouble to make Internet specialist organizations (ISPs) team up. Since the spoofers could spread over each side of the world, a solitary ISP to send its own traceback framework is practically unimportant. Be that as it may, ISPs, which are business elements with serious connections, are for the most part absence of express monetary motivating force to help customers of the others to follow aggressor in their oversaw ASes.

Since the sending of traceback instruments isn't of clear gains however obviously high overhead, to the best information on creators, there has been no sent Internet-scale IP traceback framework till now. Thus, in spite of that there are a great deal of IP traceback components proposed and an enormous number of parodying exercises watched, the genuine areas of spoofers despite everything stay a puzzle.

Given the troubles of the IP traceback systems arrangement, we are thinking about another course: following the spoofers without sending any extra instrument. In another word, we attempt to reveal the area of spoofers from the follows created by existing broadly received capacities on product switches when mocking assaults occur.

Rather than proposing another IP traceback system with improved following ability, we propose a novel arrangement, named Passive IP Traceback (PIT), to sidestep the difficulties in

organization. Switches may neglect to advance an IP ridiculing parcel because of different reasons, e.g., TTL surpassing. In such cases, the switches may create an ICMP blunder message (named way backscatter) and send the message to the caricature source address. Since the switches can be near the spoofers, the way backscatter messages may conceivably reveal the areas of the spoofers. PIT misuses these way backscatter messages to discover the area of the spoofers. With the areas of the spoofers known, the casualty can look for help from the comparing ISP to sift through the assaulting parcels, or take different counterattacks. PIT is particularly helpful for the casualties in reflection based caricaturing assaults, e.g., DNS intensification assaults. The casualties can discover the areas of the spoofers legitimately from the assaulting traffic.

2. LITERATURE SURVEY

Writing study is the most significant advance in programming improvement process. Prior to building up the device, it is important to decide the time factor, economy and friends quality. When these things are fulfilled, ten subsequent stages are to figure out which working framework and language utilized for building up the apparatus. When the developers begin constructing the device, the software engineers need part of outside help. This help got from senior software engineers, from book or from sites. Before building the framework the above thought r taken into for building up the proposed framework.

To encode a message, a meeting key should initially be created by utilizing the CryptGenKey work. Calling this capacity produces an arbitrary key and returns a handle with the goal that the key can encode and decipher information. You ought to determine the encryption calculation now. Since CryptoAPI doesn't allow applications to utilize open key calculations to encode mass information, call CryptGenKey to determine a symmetric calculation, for example, RC2 or RC4, for your application.

Then again, if your application needs to encode the message so that anybody with a predetermined secret phrase can unravel the information, the CryptDeriveKey capacity ought to be utilized to change the secret phrase into a key appropriate for encryption. For this situation, CryptDeriveKey is called rather than CryptGenKey, and the ensuing CryptExportKey calls are not required.

When the key is created, other cryptographic properties of the key can be set with CryptSetKeyParam. For instance, various areas of the record can be encoded with various salt qualities, and the code mode or introduction vector can be changed. Applications can create salt qualities with the CryptGenRandom work.

In square codes, you can change the technique for encryption by setting the square code properties with CryptSetKeyParam. The accompanying table shows the code modes.

In this ECB figure mode, each square is encoded independently and no input is utilized. This implies indistinguishable squares of plaintext encoded with a similar key are changed into indistinguishable code squares. On the off chance that a solitary piece of the code square is jumbled, at that point the whole relating plaintext square is likewise confused.

Each plaintext obstruct in this CBC figure mode is encoded dependent on the code of the past square. CBC guarantees that regardless of whether the plaintext contains numerous indistinguishable obstructs, each encodes to an alternate code square. Additionally to EBC, if a solitary piece of the code square is distorted, the comparing plaintext square is likewise jumbled. Additionally, a piece in the resulting plaintext hinder in a similar situation as the first confused piece, is jumbled. In the event that there are extra or missing bytes in the code, the plaintext is confused starting there on.

3. EXISTING SYSTEM

In the existing system we try to use the dynamic routing technique for sending packets from a valid source node to the destination node. In the existing routing scheme, there is no concept like detecting and countermeasure of spoofing attack. All the existing approaches try to detect the ip spoofing attack based on the changed ip address. If there is any node failed within the router then such a node will be identified as spoofed node and there is no technique which can provide counter measure for that spoofed node in a run time manner.

3.1 LIMITATION OF EXISTING SYSTEM

The following are the limitation of existing system. They is as follows:

1. There is no method to provide counter measure for that spoofing attack.
2. Data security is very less due to Spoofing attacks
3. All the existing approaches failed in identifying Spoofed nodes during run time and provide an alternate path by using path scatter approaches.
4. All the existing approaches try to use static path identifiers and they used to send all the packets in that static predefined paths

4. PROPOSED SYSTEM

The main contribution of this paper is to provide a distributed passive IP Trace back approach in which the data is initially divided into packets and where each and every packet transmission can be overheard by a sequence of intermediate nodes that are available in the router among which the next relay is selected dynamically. The main challenge in the design of proposed PIT model is balancing the trade-off between routing the packets along the shortest paths to the destination and try to provide an alternate path at the time of traffic. If there is any spoofing attack found automatically PIT model will backscatter one step back to its origin and try to send to the destination node by choosing an alternate path.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. Avoids spoofing attacks by using PIT model.

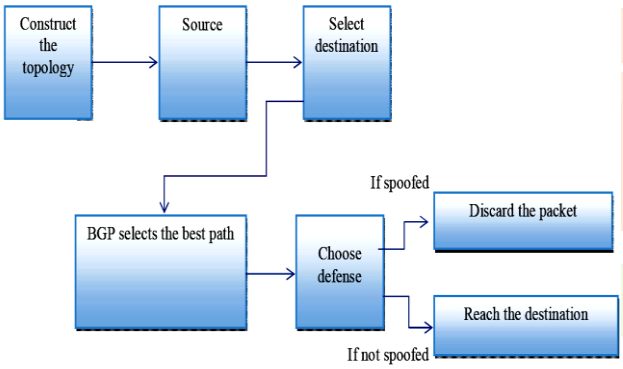
2. Packets loss will be avoided due to back scattering method as

3. IT is dynamic in nature so there is no scope of data loss if any spoofing attacks occur during transmission

4. In this proposed approach we can achieve high level of accuracy in sending the packets to the destination node.

5. It is efficient and practical method for packet delivery.

5. THE PROPOSED APPROACH



The following are the step by step procedure for the this proposed application.This is as follows:

The algorithm is given below:

Step 1: Initially we need to construct the topology

Step 2: The sender and receiver nodes are initialized with the centralized router.

Step 3: The sender try to choose a valid file and convert the data into packets and then send those packets to the router node.

Step 4: The router will receive the data packets and try to identify if there are any spoofed nodes are present in that neighbour list.

Step 5: The router will generate a best path if there is no spoofed nodes available and allow the data to be pass under that best path.,

Step 6: If the router finds any spoofed node then immediately it will backtraverse one step back and choose next alternate node for sending the packets to destination using PIT model

Step 7: The receiver verifies the received packets and try to observe if there is any attacks occurred during communication and then identify the delay time

Step 8: Exit

6. MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JSE as the chosen language in order to show the performance this proposed Mixed Stegnography. The front end of the application takes AWT,SWINGS and SECURITY PACKAGE and as a Back-End Data base we took some sample digital data collected from the PC. The application is divided mainly into following 6 modules. They are as follows:

Now let us discuss about each and every module in detail as follows:

6.1 Service Provider Module

In this module, the service provider will browse the data file, initialize the router nodes, for security purpose service provider encrypts the data file and then sends to the particular receivers (A, B, C, D…). Service provider will send their data file to router and router will select smallest distance path and send to particular receiver.

6.2 Router Module

The Router manages a multiple nodes to provide data storage service. In router n-number of nodes are present (n1, n2, n3, n4, n5…). In a router service provider can view node details and routing path details. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver. If any attacker is found in a node then flow will be send to IDS manager and router will connect to another node and send to particular receiver.

6.3 IDS Manager Module

In this module, the IDS Manager detects introducer and stores the introducer details. In a router any type of attacker (All Spoofers like source, destination, DOS Attacker) is found then details will send to IDS manager. And IDS Manager will detect the attacker type (Active attacker or passive attacker), and response will send to the router. And also inside the IDS Manager we can view the attacker details with their tags such as attacker type, attacked node name, time and date.

6.4 Receiver Module

In this module, the receiver can receive the data file from the router. Service provider will send data file to router and router will accept the data and send to particular receiver (A, B, C, D, E and F). The receivers receive the file in decrypted format by without changing the File Contents. Users may receive particular data files within the network only.

6.5 Attacker Module

In this module, there are a two types of attacker is present in the real word. One is active or insider attacker who will inject the false data within our region and other is outsider or passive attacker who will attack or inject the node from external sources during data transmission. Here in this paper we will come across the passive attacker where he can do spoofing in many ways like Bandwidth spoofing, Message or Malicious spoofing and IP Spoofing. It is clearly identified the difference of each and

every spoofing in the implementation of this project.

6.6 Performance Evaluation Module

Here in this project ,we have an performance evaluation module ,where at the end after all the data transmission is done between the sender and receiver,there may occur some attacks during transmission.So such an attacks can be examined and viewed in a graphical manner.Here we used Bar charts for comparative analysis so that it will be showing the nodes and its delay time ..Here X- Axis is represented with the sensors or nodes which help to reach the destination like N5,N6,,,N10…And also Y-Axis represents the delay in milli seconds..SO this graph will show a detailed view about the performance of our proposed algorithm

7. RESULTS

Router will deliver the file to the destination node

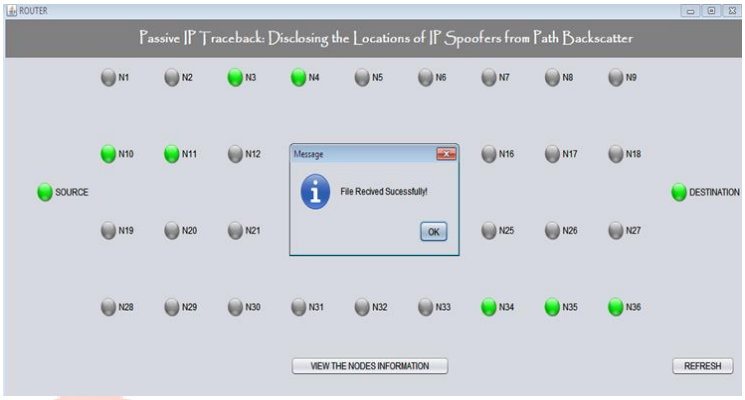


Figure . Represents the File Delivered

Destination Node receive the File

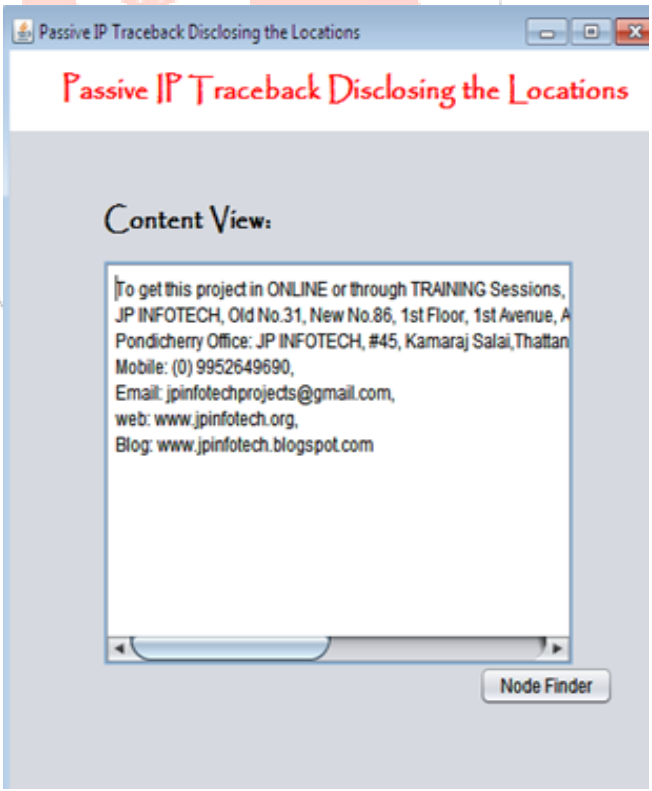


Figure . Represents the File is Received

Attacker try to create attack

Figure Represents the Attacker create attack

Attacker try to create attack

Figure Represents the File is attacked by the attacker by IPSpoofer

Data is received successfully even a node is attacked with in the network

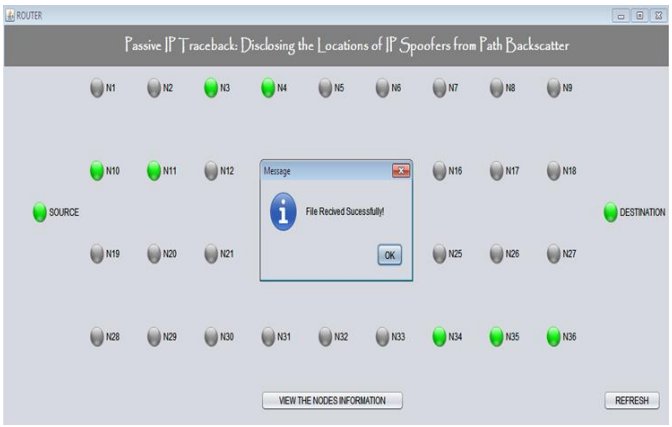


Figure Represents the Data received Successfully

8. CONCLUSION

In this proposed application we finally came to an conclusion by designing the PIT model known as Passive IP Trackback model in which if there is any Spoofing attack is found it will immediately backtraverse for one node back to its previous origin and try to send the data to valid destination with the help of other intermediate nodes. By conducting various experiments on our proposed PIT model, we finally came to a conclusion that our proposed model is very efficient in capturing the location of IPSpoofers based on path backscatter data set and as an extension we have showed the application under a simulation chart with nodes and their attack scenario is identified easily through that chart model.

9. REFERENCES

[1] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 19, no. 2, pp. 32–48, Apr. 1989.

[2] ICANN Security and Stability Advisory Committee, "Distributed denial of service (DDOS) attacks," SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006.

[3] C. Labovitz, "Bots, DDoS and ground truth," presented at the 50th NANOG, Oct. 2010.

[4] *The UCSD Network Telescope*. [Online]. Available : http://www.caida.org/projects/network_telescope/

[5] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in *Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM)*, 2000, pp. 295–306.

[6] S. Bellovin. *ICMP Traceback Messages*. [Online]. Available: http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.

[7] A. C. Snoeren *et al.*, "Hash-based IP traceback," *SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 4, pp. 3–14, Aug. 2001.

[8] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Trans. Comput. Syst.*, vol. 24, no. 2, pp. 115–139, May 2006. [Online]. Available: http://doi.acm.org/10.1145/1132026.1132027

[9] M. T. Goodrich, "Efficient packet marking for large-scale IP traceback," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 117–126.

[10] D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," in *Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, vol. 2. Apr. 2001, pp. 878–886.

[11] A. Yaar, A. Perrig, and D. Song, "FIT: Fast internet traceback," in *Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, vol. 2. Mar. 2005, pp. 1395–1406.

[12] J. Liu, Z.-J. Lee, and Y.-C. Chung, "Dynamic probabilistic packet marking for efficient IP traceback," *Comput. Netw.*, vol. 51, no. 3, pp. 866–882, 2007.

[13] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack," in *Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, vol. 1. Apr. 2001, pp. 338–347.

[14] M. Adler, "Trade-offs in probabilistic packet marking for IP traceback," *J. ACM*, vol. 52, no. 2, pp. 217–244, Mar. 2005.

[15] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," *IEEE*

Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.

[16] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 4, pp. 567–580, Apr. 2009.

[17] R. P. Laufer *et al.*, "Towards stateless single-packet IP traceback," in *Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN)*, Oct. 2007, pp. 548–555. [Online]. Available: http://dx.doi.org/10.1109/ LCN.2007.160

[18] M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, and O. C. M. B. Duarte, "A stateless traceback technique for identifying the origin of attacks from a single packet," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2011, pp. 1–6.

[19] A. Mankin, D. Massey, C.-L. Wu, S. F. Wu, and L. Zhang, "On design and evaluation of 'intention-driven' ICMP traceback," in *Proc. 10th Int. Conf. Comput. Commun. Netw.*, Oct. 2001, pp. 159–165.

[20] H. C. J. Lee, V. L. L. Thing, Y. Xu, and M. Ma, "ICMP traceback with cumulative path, an efficient solution for IP traceback," in *Information and Communications Security*. Berlin, Germany: Springer-Verlag, 2003, pp. 124–135.

[21] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in *Proc. LISA*, 2000, pp. 319–327.

[22] R. Stone, "CenterTrack: An IP overlay network for tracking DoS floods," in *Proc. 9th USENIX Secur. Symp.*, vol. 9. 2000, pp. 199–212.

[23] A. Castelucio, A. Ziviani, and R. M. Salles, "An AS-level overlay network for IP traceback," *IEEE Netw.*, vol. 23, no. 1, pp. 36–41, Jan. 2009. [Online]. Available: http://dx.doi.org/10.1109/MNET.2009.4804322

[24] A. Castelucio, A. T. A. Gomes, A. Ziviani, and R. M. Salles, "Intradomain IP traceback using OSPF," *Comput. Commun.*, vol. 35, no. 5, pp. 554–564, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366410003804

[25] J. Li, M. Sung, J. Xu, and L. Li, "Large-scale IP traceback in high-speed internet: Practical techniques and theoretical foundation," in *Proc. IEEE Symp. Secur. Privacy*, May 2004, pp. 115–129.