ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Tracking and Tracing Spoofed IP Packets Using Probabilistic Packet Marking and Passive IP Traceback

R. Vimala Devi, Bindiya. M.K

M. Tech Student, Department of CSE, SJBIT, Bangalore, India

Associate Professor, Department of CSE, SJBIT, Bangalore, India

ABSTRACT: Security is an important role in today's network. When planning, developing and deploying a network one should understand the importance of a strong security policy. A security policy defines what people can and can't do with network components and resources. There are numerous attacks perpetrated on them conspicuously when it comes to denial of service (DOS) attack. In this paper we are considering spoofing IP address. IP is an internet protocol where each and every system having a unique address and this address is used to communicate to the internet. Main purpose of our proposed system is to identify the true IP address and the source of its attacker. To accomplish this we make use of probabilistic packet marking and passive IP trace back techniques.

KEYWORDS: IP traceback, DOS attack, spoofing, probabilistic packet marking, passive IP traceback.

I. INTRODUCTION

Spoofed packet is generally a request generated by a client node for the server or another computer. The main purpose of using spoofed packets is to hide the actual uniqueness of the sender. Creating spoofed packet is not the actual technique, the real task is to achieve IP spoofing, and that is creating a forged IP address that does not actually belong to any of the computer on the Internet currently. The spoofed packet is the data that is sent from an unknown and forged IP address. Spoofed packets are primarily used in denial of services attacks and are also used as a backup or secondary option in distributed denial of service attacks where the attackers wants to overcome the server or target website with requests without giving his actual uniqueness or IP address.

Spoofed packets are created by the spoofers by modifying the information about source address in the header section of a IP packet. After modifying the numerical value and source address the attacker effectively creates a spoofed packet that appears as if it was sent from a valid machine. The server which receives the spoofed packet wills response to the address which has been altered in the IP header of the packet. In this scenario an attacker not only stay hidden but also use the full uplink of the server and utilizes bandwidth of the victim server. Spoofed packets are also used to defeat the security mechanism of a network and avoid services which are based upon IP authentication.

The main concept behind the IP traceback is to determine the correct IP address of the source from which the attacks are being launched. Although this can normally be gathered by locating the IP address field from the IP packet, regrettably the attacker can easily manipulate and change these details, thus masking its original and actual uniqueness. IP traceback can hence be classified as belonging to two different methods: proactive and reactive.

Proactive Tracking Methodology : This method would involve detecting and tracing attacks when packets are being transmitted. If packet tracing is needed, the victim can hence refer to this information to identify the attacking source. However the proactive methods can be further divided into two different proactive methods namely packet marking and packet messaging. Packet Marking: This would involve packets that contain information about each and every router that they traverse through. Therefore, this means that the receiver of the chosen packet can make use of the information held by the router to traceback packet's route to its source. It is necessary that routers can mark and sign packets without interrupting the normal packet processing.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Message Marking: In this particular approach, the different routers, through which the packets traverse through, generate and broadcast messages with call the information about the forwarding nodes that a particular packettraverse through.

Reactive Tracking Methodology : The reactive tracing method operates in a different way than the proactive one. In this approach, the tracing will only initiate when an attack has been perpetrated and following its detection. However, the several trials in developing a practical traceback algorithm and packet matching techniques have tried to resolve these dilemmas. Among those analyzed approaches are hop-by-hop tracing, IPSec authentication and monitoring traffic patterns matching.

II. RELATED WORK

Vamsi Paruchuri et.al [1], in his paper he have proposed a new scheme which is PPM scheme called TTL-based PPM (TPM) scheme, in which each packet that has to be transmitted is marked with a probability inversely proportional to the distance travelled by the packet so far. Hence, packets that have to travel longer distances are marked with higher probability, compared to those packets that have to travel for shorter distances.

Akash mittal et.al [2], in this paper basically he have summarized different approaches of DDoS and its countermeasures by different methods such as Bloom Filter, Trace Back method, Independent Component Analysis and TCP Flow Analysis.

K.Sudha et.al [3], this paper proposes a multivariate correlation analysis approach to study and detect the Dos attack. The proposed system applies the design of Multivariate Correlation Analysis (MCA) to network traffic characterization and employs the principal of anomaly-based detection in attack recognition. One major complexity to shield against Distributed Denial-of-service attack is that attackers often use forged or spoofed IP addresses as the IP source address. To identify the spoofers, this paper proposes passive IP traceback (PIT) that avoid the deployment difficulties of IP traceback techniques. PIT studies Internet Control Message Protocol error messages (named path backscatter) generated by spoofing traffic, and tracks the spoofers using available public information (e.g., topology).

Hemant et.al [4], developed a behavioral distance based anomaly detection mechanism with the ability of performing on-line traffic analysis. To create accurate online traffic profiles, they have introduced a horizontal and vertical distance metrics between various traffic features (i.e., packet header fields) in the traffic data streams. The major advantages of the proposed approach lie in four aspects: (1) it is proficient and effortless enough to process on-line traffic data; (2) it make possible protocol behavioral analysis without maintaining per-fluctuate; (3) it is scalable to high speed traffic links due to the aggregation, and (4) using a variety of combinations of packet features and measuring distances between them.

III. PROPOSED SYSTEM

This section explains the architecture of the proposed system. It mainly includes:

a. Network Initialization

Network initialization is to specify various network parameters before actually starting a network. The parameters include the working channel, the network identifier, and network address allocation.

b. Source and Destination nodes selection

In our proposed system, users will select the source and destination.

c. Path Selection

In path selection, we find shortest distance between identified source and destination nodes in the network. Modified Dijkstra's algorithm find shortest path from single source node to single destination node. Dijkstra's algorithm assigns tentative distance value to each node in network. Initially a value of zero is assigned to source node and infinity to other nodes. It divides the nodes into two sets: - tentative and permanent.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

d. Passive IP Traceback

Here a source node sends an acknowledgement to all its nodes in path selected in order to reach its destination. When a packet is arrived at a particular node, it sends back an acknowledgement to the sender. After receiving the acknowledgement it sends to next nodes. when it encounter spoofing node there will be delay to receive the acknowledgement and receives two packets from original node and spoofing node.

e. Probabilistic Packet Marking

In probabilistic packet marking, at each node in the path selected it checks the field in the packet whether it is marked by the sender or not, if marked then it sends the packet to the next node. If not marked it sends the notification.

In our proposed method we are combining passive Ip traceback and probabilistic packet marking methods. When we receive a packet from the source node first it identifies the marked field, if present sends the acknowledgment back to the sender. i.e.,we are simultaneously marking and tracing the packets received by the node and considers that packet as valid one. If the identity is absent in any of the packet, then it is marked as invalid identifying spoof node.

- *Complementary Cumulative Distribution Function (CCDF)*

A CCDF curve shows how much time the signal spends at or above a given power level. The power level is expressed in dB relative to the average power. A CCDF curve is basically a plot of relative power levels versus probability.

Each CCDF is constructed from a set of input values that is consistent with all available information. The assignment of distributions to individual inputs and the propagation of these distributions to the distribution of CCDF curves provid ea representation of the uncertainity in the final outcome is a CCDF. Applying another way, the distribution of CCDF curves provides a measure of the confidence with which the outcome of the risk assessment can be estimated. A tight grouping of CCDF indicates a high confidence in the estimated location of the CCDF of interest; conversely, a wide spread in the CCDF curves indicates a low confidence in the estimated location of this CCDF. Mathematically CCDF can be explained with a set of data having the probability density function (PDF). To obtain the Cumulative Distribution Function (CDF), the integral of the PDF is computed. Then inverting the CDF results in the CCDF. It concludes that the CCDF is the complement of the CDF or CCDF=1-CDF.

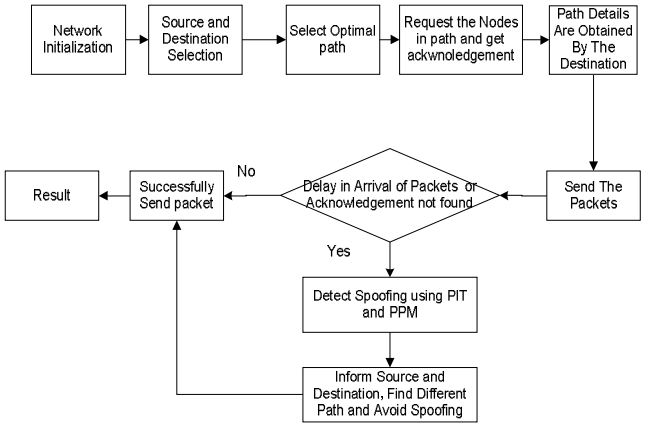

Figure 1: Proposed Architecture

IV. RESULTS

This section explains the Output of each phase in our proposed System.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

- The Probability of Accurate Locating

Probability of accurate locating the attacker is obtained using

$$E(P_{LF-accurate}) = \frac{N-1}{N} * \frac{\lambda + b_d}{1 + \delta_{ef}} \qquad (1)$$

This form gives the probability of accurate locating. If the power-law becomes stronger, λ will get larger and δ_{ef} will get smaller. Then the probability of accurate locating will be larger.

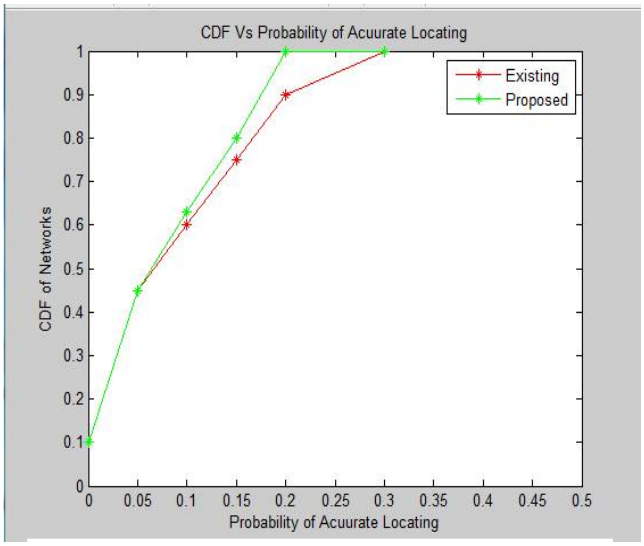

Figure 4: Graph for existing vs. proposed system

IV. CONCLUSION

It is long known attackers may utilize fashioned source IP location to cover their real areas. To capture the spoofers, various IP traceback mechanisms have been proposed. In this paper we have presented a new technique, by combining IP traceback and probabilistic packet marking method both together to achieve the security policy. Our experimental results shows that proposed method have traced the spoofers and produces more accurate results compared to existing methods.

REFERENCES

[1] Vamsi Paruchuri, Arjan Durresi and Sriram Chellappan*" TTL based Packet Marking for IP Traceback".
[2] Akash Mittal , Prof. Ajit Kumar Shrivastava , Dr. Manish Manoria, " A Review of DDOS Attack and its Countermeasures in TCP Based Networks" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011
[3] K.Sudha Deepthi1 " A Novel Passive IP Approach for Path file sharing through Backscatter in Disclosing the Locations" " International Journal of Computer Science & Engineering Survey (IJCSES) October'2015
[4] Hemant Sengar" Online Detection of Network Traffic Anomalies Using Behavioral Distance"
[5] Vamsi Paruchuri, Arjan Durresi and Sriram Chellappan "On the (in)effectiveness of Probabilistic Marking for IP Traceback under DDoS Attacks"
[6] Raju M. Shingade, "Detection of Spoofing attackers in wireless network", International Journal of Innovative Research in Advanced Engineering,Vol. 1 , pp 124-134,May 2014.
[7] Aman Shekhar, "Passive IP Traceback: Disclosing the Locations of Man in the Middle from Path Backscatter", International Journal of Computer Science Trends and Technology (IJCST) – Vol. 3 No.5, Sep-Oct 2015.
[8] W. Caelli, S. Raghavan, S. Bhaskar, and J. Georgiades, "Policy and law: denial of service threat," in An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks, pp. 41–114, 2011.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

[9] A. Belenky and N. Ansari, "Ip traceback with deterministic packet marking," IEEE communications letters, Vol. 7, No. 4, pp. 162–164, 2003.
[10] M.-H. Yang and M.-C. Yang, "Riht: A novel hybrid IP traceback scheme," IEEE Trans. Inf. Forensics Security, Vol. 7, No. 2, pp. 789–797, Apr. 2012.
[11] R.H. Campbell, Z. Liu, M.D. Mickunas, P. Naldurg, and S. Yi. Seraphim: Dynamic Interoperable Security Architecture for Active Networks. In Proceedings of IEEE OPENARCH 2000, March 2000.
[12] N. Johnson, Z. Duric, and S. Jajodia. Information Hiding: Steganography and Watermarking - Attacks and Countermeasures. Kluwer Academic Publishers, February 2001.