IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IoT Networks Protection against IP Spoofing Attacks via IP Trace-Back Detection Technique

Ms.Shilpa B.Sarvaiya
Department of Computer Science
Vidyabharati Mahavidyalaya, Amravati
sarvaiya.shilpa@gmail.com

Dr.D.N.Satange
Department of Computer Science
Narsamma Hirayya Arts Commerce & Science, Amravati
dineshnsatange@rediffmail.com

ABSTRACT

In 2050,every electronics devices getting to be controlled and can we operate through the mobile phones.So,for every second data will be stored and retrieved.IoT architecture mostly consist of sensors which are connected to IoT board so,this particular IoT board is called as Node.The numbers of Node will be connected into single network which will be called as IoT Networks.Whole data will be passed through this IoT Networks so,may their will be a chance to the inturder to hack this networks through IP Spoofing Attacks which may cause a big loss.So,by applied a novel solution approach for detecting and preventing IP Spoofing attacks it is possible to avoid this loss. This paper fall into the problem of IP spoofing attacks give out by IoT devices and comes up with an authentication mechanism which uses Hop by Hop tracing to protect against such types of attacks without exhausting the devices in case of data transmission, processing capacity and depository. The trusted host identification is the best solution to avoid various IP spoofing attacks.

Keyword: Attacks, IP Address, IoT (Internet of Things), IP Spoofing, IP Trace-Back, Packet Filtering.

1. Introduction

This paper studies understandable idea of how IP spoofing mechanism is done and its detection techniques in the IoT Network communication. The hardest attacks among all the security problems is Dos (Daniel of service attacks) because this attack is much unidentified difficult to locate and difficult to prevent as well. Even the person who has the basic knowledge about networking can attack and enter into the untrustworthy networks with the help of some tools this type of attacks is easily spread. Many web sites are hacked before the IP trace-back was implemented, which include some famous web sites yahoo and more [1].

The fundamental idea of this DDoS attack is or copying someone else IP address, this IP of the trusted host can be copied from the attacked packets. It is very hard to find, out the source IP of the attackers because internet is stateless this is called IP trace-back. There are many IP trace-back schemes which have their own advantages and disadvantages. Some are time tracking solution and some are most promising solutions. According to our survey on IP trace-back we found some significant solution for the IP spoofing, and some of the avoiding methods. This method describes how to hide individual IP address and also how to be unknown on the internet. In IP spoofing attack, malicious node disguise their real location from victim nodes using fake IP (Internet Protocol) address, which is a major disadvantage in present internet architecture. This crime in the internet is controlled by deploying the technology named as Internet Protocol (IP) Track-back technique. We can trace back the approximate source IP addresses where spoofing is initialized. This packet tracing technique can be implemented during the attack or after the attack [2].

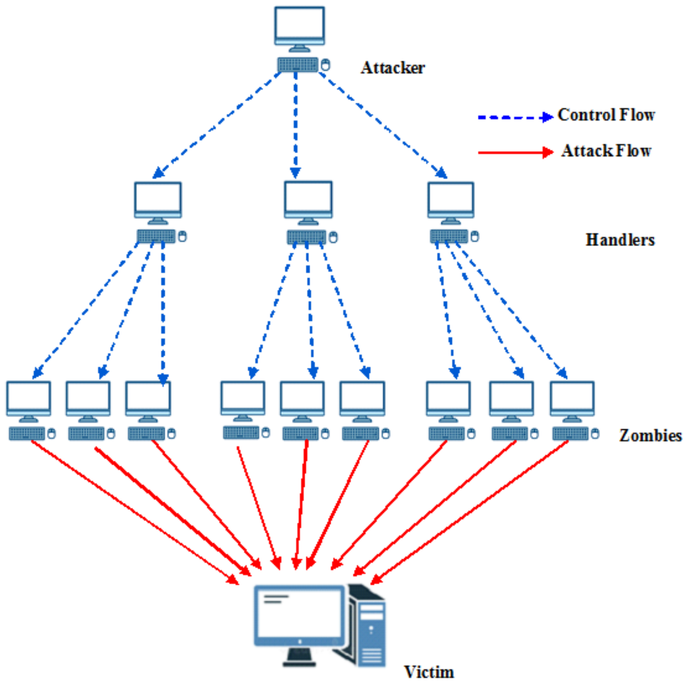


Figure 1: A DDoS Attack Architecture Depicting Control Flow and Attack Flow

2. IP Spoofing

IP spoofing is copying or making a duplicate of somebody else IP who is trusted host of the victim inside the private network. The packet filter router allows the trusted host by verifying the source IP address who is not a trusted host; attacker pretends to be trusted host. Thus an attacker enters into the private network without having an authorization [3].

IP spoofing is used to gain unauthorized access to a computer. The attacker forwards packets to a computer with a source address indicating that the packet is coming from a trusted port or system. Attackers must go through some complicated steps to accomplish the task [4]. They must:

- Attacker selects a host (Target/Victim).
- Identify host that has trust relation with target.
- Disable the trusted host, sampled the target' TCP sequence.
- The trusted host is impersonated and the ISN forged.
- Attacker successfully connects to the server.
- Attacker executes commands and controls the victim system.

Systems 'A' act like a System 'B' by sending B's IP address instead of its own IP address the reason for doing this is that systems tend to function within groups of other trustworthy systems. This trust is implemented in a one-to-one manner; system A trusts system 'B'.

IP spoofing occurs in the following manner:

If System 'A' trusts System 'B' and System 'C' spoofs System 'B', then System 'C' can gain otherwise denied access to System 'A'.

This is all made possible by means of IP address authentication, and if the packets are coming from external sources poorly configured routers [4].

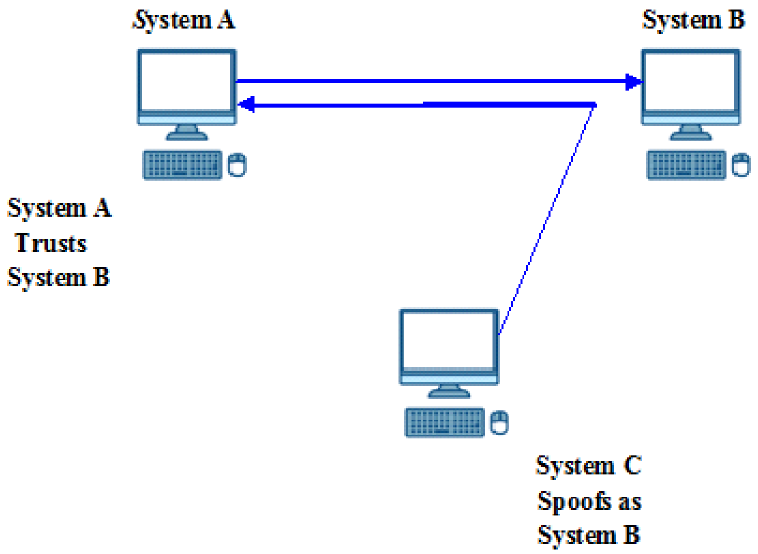


Figure 2: IP Spoofing Mechanism

3. IP Spoofing Detection Technique

This paper primarily focuses on IP spoofing attack, which is among one of the Denial of Service (DoS) attack. IP spoofing attack is one among the challenging issue in the internet. This trackback technique proposes a novel features to track the origin of spoofers with best tracking performance than existing techniques, as an enhancement to existing trackback techniques this IP trackback needs to add very small amount of packets, which would load the routers moderately to accomplish the objective of tracking to detect the spoofers in a vast internet. The enhanced system IP trackback mechanism achieves the objective of accomplishing best possible results on trackback although when router is loaded at its maximum. DDoS defence motivates this trackback technique [5].

3.1 Hop by Hop Tracing:

Hop-by-hop tracing program are used to log the information to the closest router to the victim. If the hop-by-hop program detects any attacker or unauthorized packet it sends the packets to the upstream router. If the router detects the unauthorized packets continuously the upstream router the packets to the corresponding upstream router, if this process is still repeating the last upstream router which contains the spoofed packets goes on by sending the packets to corresponding upstream router until the program reaches the source IP of the attacker. In hop-by-hop router if there are more hop/routers in the program the time consuming of the program is also more, this process will take more time to trace, sometimes because of long tracing important information about tracing might be lost. So to reduce the time period of tracing the source IP, there is a concept called overlay networking which is built by introduced tunnels routers in between the end router and tracking router, in this program router uses the special tracing router and edge router to trace the source IP also save the time of tracing and there is no loss of packet information in the overlay network [6].

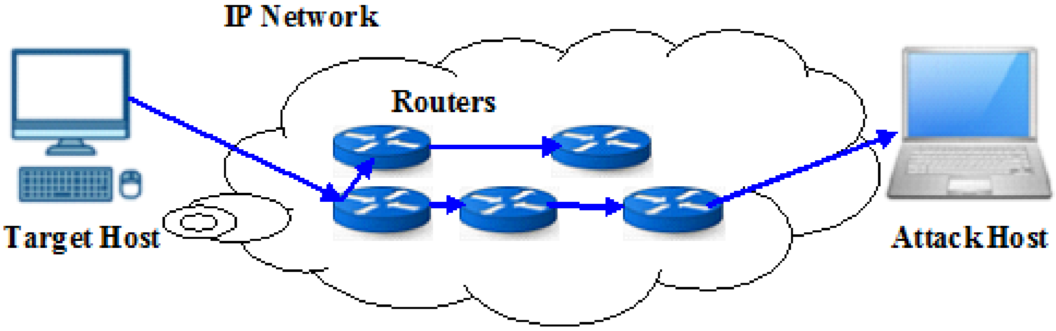


Figure 3: Hop-by-Hop Tracing

In Hop-by-Hop tracing, a tracing tool logs into the router closest to the attached host and monitoring the incoming packets. If the tool detects the spoofed packet, it logs into upstream routers and monitors packets [7].

4. Novel Solution for IP Spoofing Attacks

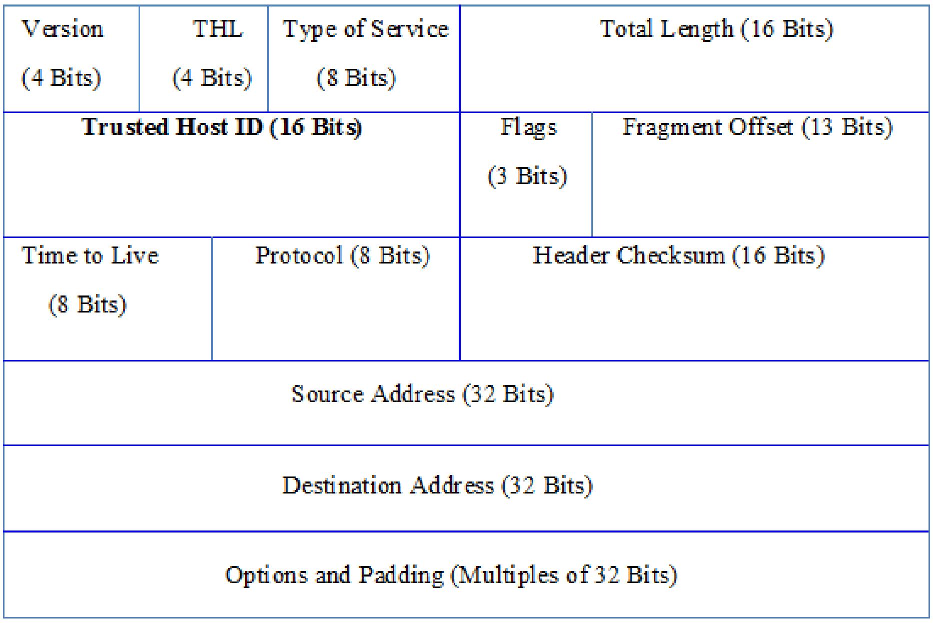
This is a novel solution that is both efficient and simple by which gateway routers on the destination network can detect and block spoofed packets. The solutions that are based on information currently found in the headers of TCP/IP packets are inadequate to protect network hosts against IP spoofing attacks [1]. Some additional information needs to be considered along with the source IP address for authentication. For this purpose we have included additional Trusted Host ID (TID) information that is unique to each user [8].

4.1 Trusted Host Identification

The trusted host identification is calculated through the following steps:

- The source address and the destination address are XORed to form an edge address.
- A 16-bit hash is computed for the edge address.
- Multiplicative inverse of the hash is calculated using Gallus Field (GF) (216) by a periodically changing primitive irreducible polynomial.

Since the edge routers observe all the outgoing traffic of the network therefore they are the best candidates to mark the packets. Each outgoing packet is marked with the TID by the egress router of the source network. At the destination network the ingress router is responsible for the processing and verification of the TID. The source and destination end routers periodically update each other on the primitive polynomial being used for each source-destination pair. If the TID computed on the destination ingress router does not correspond to the marked TID in the identification field of the packet, it is considered as spoofed and is discarded. If the TID is matched it is accepted as authenticated. This ensures that the source host lies within trusted source subnet [9]. The strength of this solution lies in the changing of the primitive irreducible polynomial. Moreover, since the computation of the TID is a complex function involving multiple operations therefore it is difficult to spoof. This could result in the overwriting of important upper layer header information. Therefore we have proposed that in our TID approach the information should be placed in the identification field [10].



<table>
<tr><td colspan="1">Version
(4 Bits)</td><td colspan="1">THL
(4 Bits)</td><td colspan="2">Type of Service
(8 Bits)</td><td colspan="4">Total Length (16 Bits)</td></tr>
<tr><td colspan="4"><b>Trusted Host ID (16 Bits)</b></td><td colspan="1">Flags
(3 Bits)</td><td colspan="3">Fragment Offset (13 Bits)</td></tr>
<tr><td colspan="2">Time to Live
(8 Bits)</td><td colspan="2">Protocol (8 Bits)</td><td colspan="4">Header Checksum (16 Bits)</td></tr>
<tr><td colspan="8">Source Address (32 Bits)</td></tr>
<tr><td colspan="8">Destination Address (32 Bits)</td></tr>
<tr><td colspan="8">Options and Padding (Multiples of 32 Bits)</td></tr>
</table>

Figure 4: IP Header with TID Field

However the selection of this field also comes with certain issues. The basic problem is that it only works for packets that are not fragmented. However recent research has proved that most of the packets in the Internet are not fragmented [11]. The second problem lies with the size of the identification field. It is a 16-bit field therefore it only allows 2^{16} possible TIDs each of length 16 which are vulnerable to exhaustive search and brute force guessing. To overcome this we have embedded Trust Host Identification (THI) functionality [12].

5. Analysis and Discussion

The goal of IP trace back is to reconstruct the attack tree which is rooted at the victim and com-posed of the attack paths from all of the attackers to the victim. Therefore, in order to track multiple attackers in a DDoS attack, the trusted host identification approach needs a mechanism to classify the routers in different attack paths.

The first approach is to XOR each node forming an edge in the path with each other. Node a inserts its IP address into the packet and sends it to b.Upon being detected at b (by detecting a 0 in the distance), b XORs its address with the address of a.

IP spoofing is one of the major security concerns. It is the basic technique employed in most of the highly prevalent attacks. IP spoofing is difficult to prevent due the inherent security weaknesses in the current TCP/IP design specifications. Existing solutions include filtering techniques, encryption and authentication. We have suggested one potential solution that involves modifications to the current IP header fields. Additional information about the host, referred to as the TID, is encoded in the identification field. This information provides a means to verify the authenticity of the source of the packet. Deployment of solution is suggested on the edge routers of the source and destination addresses.

6. Conclusion

In our conclusion is proposed to use trace back the source IP techniques for detecting spoofing attacks in wireless networks. Our approach can both detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers while trusted host identification and eliminate them. Determining the number of adversaries is a particularly challenging problem. The above IP-Back technique can help to protect your network from attack.To further improve the accuracy of determining the number of attackers present in the system.

7. References

1. Santhosh KR,Fancy C, “ Identifying Attackers Location VIA IP-TraceBack”,International Journal of Pure and Applied Mathematics,Vol.118 No.20,PP. 4515-4522 ISSN: 4515-4522,2018.

2. Sarika Sahni,Pankaj Jagtap,“ A Survey of Defence Mechanism against IP Spoofing”,Vol.4,Issue 7, PP.20-27 ISSN:3297-2007,July 2017.

3. Jaeerahmad Indikar, Irfan Bagawan, “Vindictive IP Trackback: Revealing the Area of IP Spoofers with Efficient Tracking”, International Journal for Scientific Research & Development”, Vol.6 Issue 05, PP. 297-299 ISSN: 2321-0613, 2018.

4. Jia-Ning Luo,Ming-Hour Yang, “ An Improved Single Packet Trackback Scheme for IoT Devices”, Journal of Internet Technology,Vol.20 No.3 PP.887-890,2019.

5. Huda Basim Said,Turkan Ahmed Khaleel, “ An Improved Strategy for Detection and Prevention IP Spoofing Attack”, International Journal of Computer Applications,Vol.182 No.9,PP.28-31 9,August 2018.

6. Madhurakshi B.S,Mahesan K.V, “ Identify the Attacked Information from the Spoofers by using Passive IP Trackback(PIT) Method”, International Journal of Engineering Science and Computing,Vol.7 Issue No.8 PP.14707-14714 August 2017.

7.Archana K C,Harini N,“ Mitigation of Spoofing Attacks on IoT Home Networks”, International Journal of Engineering and Advanced Technology(IJEAT),Vol.9 Issue-1S, PP.240-245 ISSN:2249-8958,October 2019.

8. S.Uma Mageshwari, R.Santhi, “Implementation of ARP Spoofing for IoT Devices Using Cryptography AES and ECDSA”, International Journal of Recent Technology and Engineering (IJRTE), Vol.8, Issue-2S11 PP.2889-2893. ISSN: 2889-2893, September 2019.

9. Hinna Hafeez,Tayyaba Khalil, “ IP Spoofing and Its Detection Techniques “International Journal of Scientific and Research Publications,Vol.7,Issue11 PP.24-28 ISSN:2250-3153,November 2017.

10. S.Rajashree,Soman K.S.,Dr.Pritam Gajkumar Shah, “ Security with IP Address Assignment and Spoofing for Smart IoT Devices”,Vol.1 Issue 2 ISSN:5386-5314 PP.1914-1918 IEEE 2018.

11. K.Vijayakumar,Achyut Rai,G.Sethil Kumar et al., “ A two-way Approach for Detection and Prevention of IP Spoofing Attacks”, ISSN: 7354-4007,PP.01-08,In AIP Conference Proceedings,06 November 2020.

12. Reem K.Alqurashi,et al., “ Detection of IP Spoofing Attack”, International Journal of Engineering Research and Technology(IJERT) ,Vol.13 No.10,PP.2736-2741,ISSN:0974-3154, 13 October 2020