IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 3, March 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 3, March 2022 ||

| DOI:10.15680/IJIRSET.2022.1103122 |

Passive IP Traceback: Disclosing the Locations of IP Spoofers from Path Backscatter

Mr. Rushikesh Ratan Palve [1], Prof. Pingle Suvarna Digambarrao [2]

PG Student, Dept. of Computer Science and Engineering, PES College of Engineering, Aurangabad (MS), India[1]

Associate Professor, Dept. of Computer Science and Engineering, PES College of Engineering, Aurangabad (MS), India [2]

ABSTRACT: IP spoofing, or attackers initiating attacks using falsified source IP addresses, has long been recognized as a critical Internet security issue. It's long been known that attackers can hide their true locations by using counterfeit source IP addresses. Several IP trace back procedures have been proposed in order to catch the spoofers. However, due to implementation difficulties, an IP trace back solution has not been extensively used, at least at the Internet level. As a result, the spoofers' mist has never dispersed. Passive IP trace back (PIT) is a technology proposed in this research that avoids the deployment challenges of IP trace back solutions. PIT looks into Internet Control Message Protocol error messages (also known as path backscatter) caused by spoofing traffic and tracks down the spoofers using publicly available data (e.g., topology). PIT may find the spoofers in this method without requiring any deployment.

KEYWORDS: IP Spoofing, Passive IP Trace back (PIT), Path Backscatter, denial of service (DoS).

I. INTRODUCTION

Malicious packet dropping attack during data transfer over network is a major security concern to data traffic in sensor networks, since it limits legal network throughput and may obstruct the propagation of critical data. Dealing with this assault is difficult since the sensor network's unstable wireless connection feature and resource limits may cause communication failure, leading to an incorrect conclusion about the presence of such an attack. IP spoofing, which refers to attackers using falsified source IP addresses to launch attacks, has long been recognized as a severe security issue on the Internet. Attackers can avoid exposing their real locations, boost the effect of their attacks, or conduct reflection-based attacks by using addresses that are assigned to others or not assigned at all. IP spoofing is used in a number of well-known attacks, including SYN flooding, SMURF, DNS amplification, and so on. A DNS amplification attack that badly harmed a Top Level Domain (TLD) name server's service. Despite widespread belief that DoS assaults are launched via botnets and that spoofing is no longer important, the ARBOR research presented at the NANOG 50th meeting reveals that spoofing is still important in observed DoS attacks. Spoofing activities are still common, according to backscatter messages intercepted by the UCSD Network Telescopes [1].

II. LITERATURE SURVEY

Using addresses that are issued to others or not assigned at all, attackers might avoid exposing their real locations, boost the effect of assaulting, or launch reflection based assaults. There have been a lot of network assaults. Collection of provenance is impossible. And it's not feasible in current base station networks. Limited scalability and efficiency It does not solve security problems and is only applicable to a limited number of network use cases. Despite widespread belief that attacks are launched from bonnets and that spoofing is no longer important, evidence suggests that spoofing is still important in observed IP attacks. Existing systems are having following disadvantages [2].

- It is not more secure. It does not deal with malicious attacks.
- It is infeasible for sensor networks where the paths may change due to several reasons.
- It is not realistic in sensor networks.
- Low efficiency and scalability.
- It does not address security concerns and is specific to some network use cases.
- Spoofing actions are still being closely tracked based on the backscatter messages from UCSD Network Telescopes [3].
- At least two significant problems must be overcome in order to construct an IP traceback system on the Internet. The first is the cost of implementing a routing system with a traceback capability. The second issue is how difficult it is to get Internet service providers (ISPs) to work together.
- Because spoofers might spread to every corner of the globe, it's essentially pointless for a single ISP to set up its own traceback system.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 3, March 2022 ||

| DOI:10.15680/IJIRSET.2022.1103122 |

- Since the deployment of traceback mechanisms is not much clear.

III. PROPOSED SYSTEM

Data is transmitted from a source node to a destination node in the proposed system, which proposes a lightweight approach for securely transmitting sensor data provenance and uses hash functionality for data aggregation check. It also expresses the issue of secure data transfer in sensor networks. In addition, the system suggests using an in-packet Bloom filter (iBF) for provenance encoding. The Hash Conversion technique was extended by the proposed system. Malicious forwarding sensor nodes stage packet drop attacks, which it detects. The data value is updated at each intermediary node in an aggregation architecture, making maintaining the relationship between provenance and intermediate data a critical concern [4]. Making the provenance encoding process dependent on partial aggregation results (PAR) and appending each PAR to the packet to check the data-provenance binding at the BS [5] is a simple solution. As a result, the aggregate verification can only succeed if both the data and the provenance are sent without interruption. The system architecture is depicted in Figure 1..

- **Network Formation**

A wireless sensor network is made up of a number of sensor nodes and a base station (BS) that collects network data. After deployment, each node sends information about its neighbours to the base station. Each sensor generates data on a regular basis [6]and sends it to the base station. In the intermediate processing nodes, data from numerous sources is combined [7]. For the attacks, the hostile adversary may bring.

- **Provenance Model**

The data's origin is shown as a straightforward path. The intermediate nodes combine their data with that of their neighbours and then send it to the base station. Bloom filters are used to transport data from sensor nodes with provenance [14]. As a result, the intermediary nodes combine the provenance and send it to the base station.

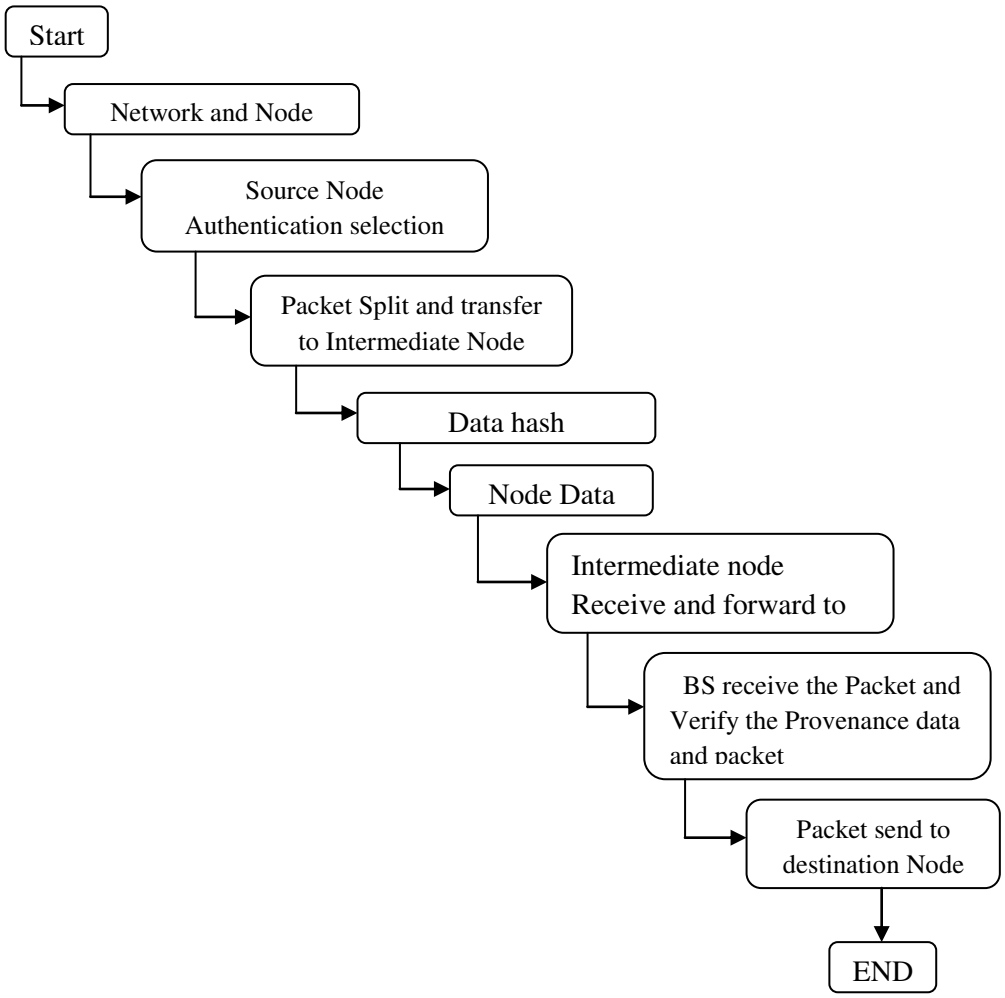

Figure 1 System Architecture

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 3, March 2022 ||

| DOI:10.15680/IJIRSET.2022.1103122 |

- **Data Hash Code Conversion Packet Drop Attack**

The Source and Network Authentication Processes have been confirmed while entering this process. The node data information will next be transformed into a hash code. The packet data will be transformed to hash code data using the hash() code function [9]. Using the SHA method, we obtain the hash key for our data and save it in the Network Database [13], after which the pocket data is forwarded to intermediate nodes, and finally the data is received by the base station.

- **Data Aggregation in Base Station**

While you're working on the provenance verification, The data will be obtained from many sources, and the packet data will be encrypted. Collection gets the nodes in the data path, while Verification includes data path, packet drop attack, and bloom filter modification. The base station [10] has received the encrypted packet. The base station will receive and decrypt the information. The original data is stored in the packet data, and the BS server verifies the user data hash key; if the key is right, the data is received by the BS server; otherwise, the data is modified by the attackers. The provenance system is checked and secured in this way, and the Spoof IPs are recognised [12].

- **Data Send to Destination Node**

The packet data was successfully sent to the base station, after which it was forwarded to the client machine via a network socket connection [11]. If an attack occurs while data is travelling between these networking systems, the node data will notify you and the file will not be moved to the destination node.

IV. CONCLUSION

The system has provided a light-weight provenance encoding and decoding strategy for this project. Bloom filters are used in this system. An in-packet Bloom filter (iBF) provenance-encoding technique was also presented. The restricted storage, energy, and bandwidth limits of sensor nodes present significant hurdles in recording provenance for each packet. As a result, a lightweight provenance solution with little overhead is required. In addition, sensorsoften operate in an untrustworthy environment where they may be attacked. As a result, security concerns including as confidentiality, integrity, and provenance freshness must be addressed. Modern networks are bi-directional, allowing sensor activity to be controlled. Military uses such as battlefield surveillance sparked the creation of wireless sensor networks, which are now utilised in a variety of industrial and consumer applications, including industrial process monitoring and control, machine health monitoring, and so on. Only authorised parties can process and confirm the integrity of provenance using this approach. Finally, the outcome demonstrates that the proposed procedure is safe. It also provides provenance secrecy, integrity, and freshness.

REFERENCES

[1] Guang Yao, Jun Bi and Athanasios V. Vasilakos, “Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter”, IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015, pp. 471-483.

[2] H. Lim, Y. Moon, and E. Bertino, “Provenance-Based Trustworthiness Assessment in Sensor Networks,” Proc. Seventh Int’l WorkshopData Management for Sensor Networks, pp. 2-7, 2010.

[3]. I. Foster, J. Vockler, M. Wilde, and Y. Zhao, “Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation, ” Proc. Conf. Scientific and Statistical Database Management, pp. 37-46, 2002

[4] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer,“Provenance-Aware Storage systems,” Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.

[5] Y. Simmhan, B. Plale, and D. Gannon, “A Survey of Data Provenance in E-Science,” ACM SIGMOD Record, vol. 34, pp. 31-36, 2005.

[6] R. Hasan, R. Sion, and M. Winslett, “The Case of the FakePicasso: Preventing History Forgery with Secure Provenance,”Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14,2009.

[7] S. Madden, J. Franklin, J. Hellerstein, and W. Hong, “TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks,” ACM SIGOPS Operating Systems Rev., vol. 36, no. SI, pp. 131-146, Dec. 2002.

[8] K. Dasgupta, K. Kalpakis, and P. Namjoshi, “An Efficient Clustering Based Heuristic for Data Gathering and Aggregation in SensorNetworks,” Proc. Wireless Comm. and Networking Conf., pp. 1948-1953, 2003.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 3, March 2022 ||

| DOI:10.15680/IJIRSET.2022.1103122 |

[9] S. Sultana, E. Bertino, and M. Shehab, "A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversariesin Sensor Networks," Proc. Int'l Conf. Distributed Computing Systems (ICDCS) Workshops, pp. 332-338, 2011.
[10] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, "Summary Cache: AScalable Wide-Area Web Cache Sharing Protocol," IEEE/ACMTrans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.
[11] A. Kirsch and M. Mitzenmacher, "Distance-Sensitive Bloom Filters,"Proc. Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006.
[12] C. Rothenberg, C. Macapuna, M. Magalhaes, F. Verdi, and A. Wiesmaier, "In-Packet Bloom Filters: Design and Networking Applications," Computer Networks, vol. 55, no. 6, pp. 1364-1378, 2011.
[13] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof Sketches:Verifiable In-Netwok Aggregation," Proc. IEEE 23rd Int'l Conf.Data Eng. (ICDE), pp. 84-89, 2007.
[14] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks," IEEE Trans. Information Forensicsand Security, vol. 7, no. 3, pp. 1040-1052, June 2012.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details