

Computer Network Secure Communication and Encryption Algorithm

Janani J, Associate Professor Dr, S R Raja

Master of Computer Application,
Centre for Open and Digital Education, Hindustan Institute of Technology and science, Chennai, India

Abstract- Due to the continuous progress of Internet technology, computer network communication service has replaced the traditional short message service and multimedia message service. In order to ensure the security of the instant messaging system, some advanced security encryption algorithms are used in the communication system to prevent attacks and information leakage. By using encryption algorithms, the network security research based. Our system operates on a network of nodes, where each node plays a crucial role in ensuring the security and integrity of transmitted data. The SHA-256 algorithm is employed for generating hash values, providing a secure and efficient means of verifying data integrity. Furthermore, we implement AES (Advanced Encryption Standard) for file encryption, enhancing the confidentiality and privacy of sensitive information. AES is a symmetric key encryption algorithm renowned for its strength and efficiency, by combining SHA-256 for integrity checking and AES for encryption, we include Face Change Attaining methods to prevent from attackers in Face Change that can support both anonymizing real IDs among neighbor nodes and collecting real ID-based encountering information. For node anonymity, two encountering nodes communicate anonymously. Our system offers a robust defense against various cyber threats, including data breaches and unauthorized access. Prevent malicious actors from intercepting or tampering with encrypted data, our system employs advanced encryption techniques and secure communication protocols.

Index Terms- Computer, Network Security

I. INTRODUCTION

A Network Topology may consist of the no. of routers that are connected with local area networks. Thus, a router can either receive data from the nearer router or from the local area network. A border router receives packets from its local network. A core router receives packets from other routers. The no. of routers connected to a single router is called the degree of a router. This is calculated and stored in a table. The Upstream interfaces of each router also have to be found and stored in the interface table. In this scheme, during the encounter, the recipient node specifies a relay node and encrypts its real ID with the public key of the relay node. It then forwards such information to the creator. Later, after the two nodes separate, the creator routes the encountering evidence to the relay node, which decrypts the ID of the recipient node and further routes the evidence to the recipient node, thereby delivering the encountering evidence. A trusted node refers to the node that is believed to keep its private key secure (i.e., does not share it with any other nodes). Otherwise, neighbor anonymity may be broken during the encountering. This is because, when two nodes meet, each node encrypts its real ID with the public key of the relay node

and sends that to the encountered node. Then, if the relay node's private key is disclosed, the real ID is no longer safe.

Hardware Requirements

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor: 15 VGA Colour.
- Mouse: Logitech
- RAM: 512 MB

Software Requirements

- Operating system: Windows XP.
- Coding Language: JAVA
- Data Base: MYSQL

What is Secure Computing?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized

access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.



Diagram clearly explain the about the secure computing

Working conditions and basic needs in the secure computing: If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

Physical Security

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense. Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present.

Human threats are not the only concern. Computers can be compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of your computer takes account of those risks as well.

Access Passwords

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection

for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.

To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

Prying Eye Protection

Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.

Anti-Virus Software

Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer).

Firewalls

Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.

Software Updates

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities.

Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.

Keep Secure Backups

Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

Report Problems

If you believe that your computer or any data on it has been compromised, you should make an information security incident report. That is required by university policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

Benefits of Secure Computing

Protect Yourself - Civil Liability

You may be held legally liable to compensate a third party should they experience financial damage or distress as a result of their personal data being stolen from you or leaked by you.

Protect Your Credibility - Compliance

You may require compliance with the Data Protection Act, the FSA, SOX or other regulatory standards. Each of these bodies stipulates that certain measures be taken to protect the data on your network.

Protect Your Reputation – Spam

A common use for infected systems is to join them to a botnet (a collection of infected machines which takes orders from a command server) and use them to send out spam. This spam can be traced back to you, your server could be blacklisted and you could be unable to send email.

Protect Your Income - Competitive Advantage

There are a number of “hackers-for-hire” advertising their services on the internet selling their skills in breaking into company’s servers to steal client databases, proprietary software, merger and acquisition information, personnel detail set al.

Protect Your Business – Blackmail

A seldom-reported source of income for “hackers” is to break into your server, change all your passwords and lock you out of it. The password is then sold back to you. Note: the “hackers” may implant a backdoor program on your server so that they can repeat the exercise at will.

Protect Your Investment - Free Storage

Your server’s hard drive space is used (or sold on) to house the hacker's video clips, music collections, pirated software or worse. Your server or computer then becomes continuously slow and your internet connection speeds deteriorate due to the number of people connecting to your server in order to download the offered wares.

Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

What Data Should be given as Input?

- How should the data be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when errors occur.

Objectives

- Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
- It is achieved by creating user-friendly screens for the data entry to handle large volumes of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data can be performed. It also provides record viewing facilities.
- When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize in an instant. Thus, the objective of input design is to create an input layout that is easy to follow

Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system’s relationship to help user decision-making.

Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

Select methods for presenting information.

Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the

- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

II. MODULE DESCRIPTION

1. Path Selection

The path is said to be the way in which the selected packet or file has to be sent from the source to the destination. The Upstream interfaces of each router have to be found and it is stored in the interface table. With the help of that interface table, the desired path between the selected source and destination can be defined.

2. Packet Sending

One of the packets or files is to be selected for the transformation process. The packet is sent along the defined path from the source LAN to destination LAN. The destination LAN receives the packet and checks whether it has been sent along the defined path or not.

3. Preventing Nodes

Face Change can prevent malicious nodes from acquiring meaningful private information by overhearing the encountering evidence and packets transmitted between two nodes. Firstly, the encountering evidence is encrypted by a key originated from two randomly generated numbers from the two encountering nodes, which are not disclosed in the network. Then, the eavesdropper cannot understand the content in the transmitted encountering evidence. Secondly in MOSN routing, the receiver of a packet is not necessary the destination of the packet. As a result, the eavesdropper cannot determine the ID of a node based on packets it receives

4. Trust Authority (TA)

The trust authority (TA), for the corresponding service. Since those services are built upon node encountering, nodes need to collect real ID based encountering information. For example, nodes need to know whom they have met to identify proximity based social community/relationships. In packet routing, nodes need to collect the encountering information to deduce their future meeting probabilities with others.

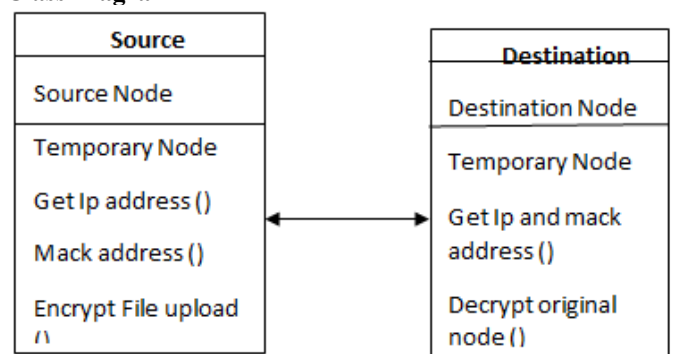
Then, a packet can always be forwarded to the appropriate forwarder Trust Authority Encryption system node encryption and file encryption using sha256 algorithm encryption original node so attackers can't file path of node where nodes send .for file encryption we are using dynamic algorithm three algorithm (AES,RSA,Blowfish) all the three algorithm encrypt file and generate private and public key to decrypt file we need both keys so that we can decrypt file by using all methods more secure both path and file.

5. Packet Routing Process

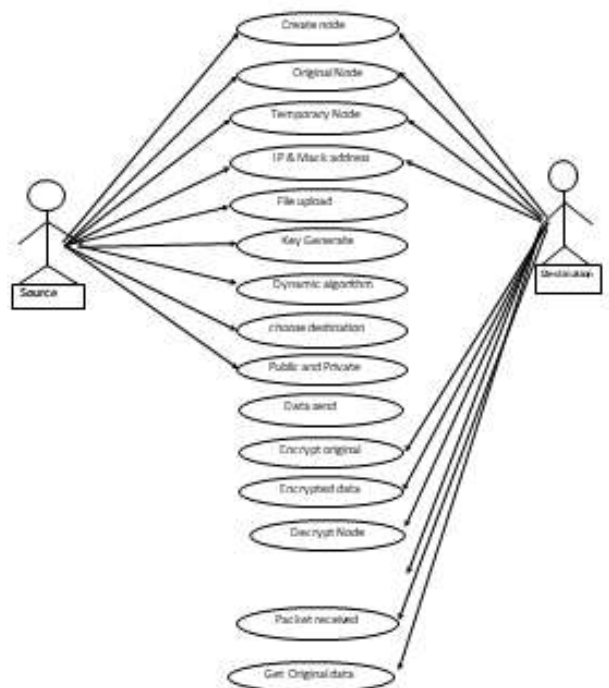
In traditional MOSN packet routing, two encountering nodes first delivers packets destined for the other node. They then compare routing utilities and forward the other node packets that the other node has a higher routing utility for their destinations.

In Face Change, neighbour node anonymity blocks the first step by preventing nodes from recognizing the destinations of their packets even when meeting them. To solve this problem, we let each node claim to have higher routing utility for itself to fetch packets for it.

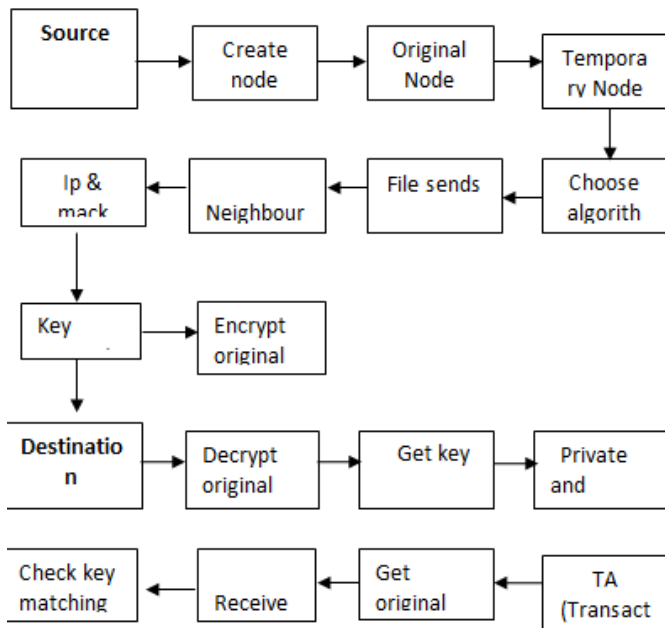
Class Diagram



III. USE CASE DIAGRAM



IV. DATA FLOW DIAGRAM



Existing System

Computer network communication service has replaced the traditional short message service and multimedia message service, and has become an irreplaceable tool in network information exchange. However, while communication brings great convenience, its message transmission process also faces many security threats, and ensuring the security of message transmission has become an urgent problem to be solved. In order to ensure the security of the instant messaging system, some advanced security encryption algorithms are used in the communication system to prevent attacks and information leakage. Existing IP traceback approaches can be classified into five main categories: packet marking, IP traceback, logging on the router, link testing, overlay, and hybrid tracing. Packet marking methods require routers modify the header of the packet to contain the information of the router and forwarding decision. Different from packet marking methods, IP traceback generates addition IP messages to a collector or the destination. Attacking path can be reconstructed from log on the router when router makes a record on the packets forwarded. Because the routers can be close to the spoofers, the path backscatter messages may potentially disclose the locations of the spoofers.

Proposed System

We propose Face Change to realize both aforementioned goals based on a key observation s. That is, disconnected nodes cannot communicate with each other directly, which makes attacking disconnected nodes almost impossible. This also means that knowing real IDs after the encountering would not compromise the privacy protection. Thus, the proposed Face

Change keeps node anonymity only during the encountering and postpone the real ID based encountering information collection to a moment after two neighbor nodes disconnect with each other. The security of the encountering evidence needs to be ensured. To encrypt node, we are using the Sha256 algorithm to improve path as strong. we are using dynamic algorithm for encrypt files and generate the public and private key RSA(Rivest-Shamir-Adleman). AES (Advance Encryption System) and Blowfish Algorithm Those Algorithm is used for dynamic encryption System Advanced extensions for sharing real IDs between mutually trusted nodes and more efficient encountering evidence collection are also proposed. Extensive analysis and experiments show the effectiveness of Face Change on protecting node privacy and meanwhile supporting the encountering information collection.

Future Enhancement

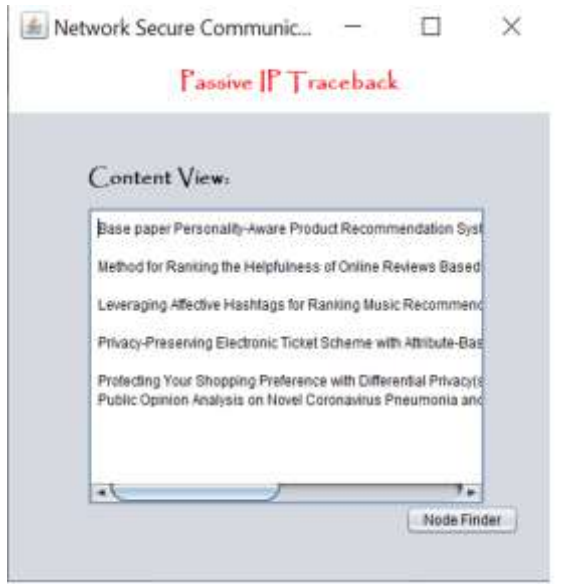
In our project the security is having perfection. We have to find the shortest path and there are many of the shortest path is ongoing, but we have done a time conception shortest path finding from which way we have to find a shortest path with time consuming. If we have 1 to 50 nodes means within the 50 nodes, we have to reach the destination by 20 nodes and by the next time we have to find a path by reaching the destination by 15 nodes. This will be indicating the time-consuming method also shortest path to reach the destination. So, using this method how we are going to finding a shortest path to reach the destination is the future enhancement.

Screenshots

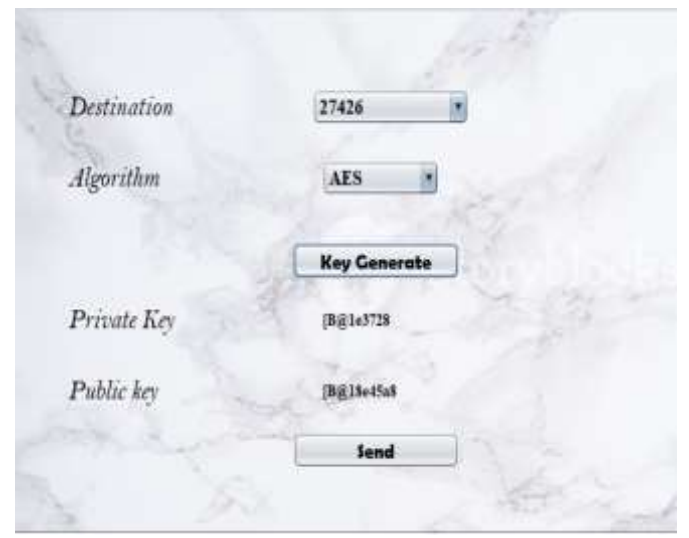




ID	NODE NAME	ATTACKER IP	DATA INTEGRITY
1	Node1	192	100%
2	Node2	192	100%
3	Node3	192	100%
4	Node4	192	100%
5	Node5	192	100%
6	Node6	192 198.178	100% data
7	Node7	192	100%
8	Node8	192	100%
9	Node9	192	100%



ID	NODE NAME	ATTACKER IP	DATA INTEGRITY
1	Node1	192	100%
2	Node2	192	100%
3	Node3	192	100%
4	Node4	192	100%
5	Node5	192	100%
6	Node6	192	100%
7	Node7	192	100%
8	Node8	192	100%
9	Node9	192	100%





V. CONCLUSION

In this article, we proposed dynamic algorithm to protect both path and files. In this paper, we propose Face Change, a system that supports both neighbor anonymity and real ID based encountering information collection in MOSNs. In Face Change, each node continually changes its pseudonyms and parameters when communicating with neighbors' nodes to hide its real ID. Moreover, file security within the network is addressed through dynamic encryption algorithms. Data encryption techniques such as Advanced Encryption Standard (AES) and RSA are dynamically applied based on file types, sensitivity levels, and contextual parameters. This ensures that files are encrypted with the most suitable algorithm, balancing security requirements with computational efficiency. Finally, the dynamic algorithm presented in this paper offers a comprehensive approach to network security, addressing both node and file security through adaptive authentication and encryption techniques. By continuously adapting to evolving network dynamics and threat landscapes, the algorithm

provides a robust defense mechanism against cyber threats, ensuring the confidentiality, integrity, and availability of network resources in modern digital environments

REFERENCES

1. S. M. Bellovin, "Security problems in the TCP/IP protocol suite," ACM SIGCOMM Compute. 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_telemeter/
5. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proc. Conf. Appl., Technol., Archit., Protocols Compute. 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. Soreen et al., "Hash-based IP traceback," SIGCOMM Compute. 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. Compute. 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. Yasar, 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. Compute. Commun. Newt.*, 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, "Center Track: An IP overlay network for tracking DoS floods," in *Proc. 9th USENIX Secure. 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 net.*, 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," *Compute. Commun.*, vol. 35, no. 5, pp. 554–564, 2012. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0140366410003804>