1

Cyber Quantum Computing (Security) Using Rectified Probabilistic Packet Mark for Big Data

Anil V. Turukmane* and Ganesh Khekare

Department of Computer Science Engineering, Parul University, Vadodar, Gujarat, India

Abstract

In recent years, denial-of-service (DoS) assaults have been a system flaw. DoS disobedience testing has become one of the most important streams in system Quantum Computing Security). This dynamic field of investigation has yielded astounding frameworks such as pushback message, ICMP take after back, and following package improvement methods. In tributary regarded informatics, the probabilistic packet marking (PPM) standard drew in considerable thinking. To begin with, the alluring purpose of this informatics follow-up approach is that it permits alterations to etch bound data on ambush packages that support chosen likelihood. After gathering a sufficient number of examined packages, the loss (or information plan centre) will construct a set of systems that offence groups crossed and, as a result, the setback will be assigned zones. The goal of the PPM algorithmic project is to demonstrate that produced outline is the same as offence graph, where relate degree attack outline is that course of action of techniques ambush packs investigated and created outline could be diagrammed by PPM algorithmic framework. The main goal of the structure is to provide a powerful approach to cope with tracking down an assailant's back IP address through a media like the internet. The system will stamp every shipment that is to be traded over the internet as indicated by the group's substance and deliver it via trade media. When it reaches its final destination, the stamping of any package is altered, and the structure is ready to be taken. The majority of PPM concerns have entailed a few issues such as loss of stamping information, issues recreating ambush routes, and low precision than on. In the first paper, we propose a dynamic probabilistic packet

**Corresponding author*: anil.turukmane21100@paruluniversity.ac.in

Romil Rawat, Rajesh Kumar Chakrawarti, Sanjaya Kumar Sarangi, Jaideep Patel, Vivek Bhardwaj, Anjali Rawat and Hitesh Rawat (eds.) Quantum Computing in Cybersecurity, (1–16) © 2023 Scrivener Publishing LLC

marking (DPPM) approach as a replacement for another upgrade reasonability of PPM. On the other hand, if you're utilising mounted checking likelihood, we propose gauging regardless of whether the package has been stamped or not, and then selecting the appropriate checking likelihood. Most of the problems with the PPM approach could be solved using DPPM. A formal examination reveals that DPPM outperforms PPM in a variety of ways. The proposed solution is useful in domains where it is important to keep track of back IP addresses while changing the package, such as cybercrime and the illegal treatment of data groups where certain basic information must be transferred. Propose a P Packet M basic end condition, which is commonly omitted or not explicitly stated in writing. Due to the new end condition, the client of a new control has more freedom to inspect the precision of the chart that has been created.

***Keywords*:** Quantum Computing (Security), Quantum Cryptography and Quantum Computing (Security), control mechanism, cyber crime, quantum attacks

1.1 Introduction

Over the last two decades, the world has seen significant advances in science and innovation that have successfully met a wide spectrum of human needs. These requests range from basic necessities like power bills and rail ticket reservations to more complex ones like force matrices for the era of violence and sharing. These advancements have raised the standard of human existence in terms of modernity and simplicity. Unexpectedly, a competing invention for negotiating Quantum Computing (Security) has evolved, with its own set of repercussions, hindering innovation. Robbery, hacking, and the blackout of private information are examples of information-related attacks. Anonymous subterranean attack networks that can efficiently assault a specific target every time are likely to be available, according to the media and many types of network Quantum Computing (Security) literature. This merely depicts a possible transition from today's attack to future attacks. Everything is on the table in the present world, from "damage and devastation" wars to "information warfare," to the negotiation of the aforementioned attack. Finally, attackers/networks that can hide are usually the ones who carry out these attacks.

The scope of attacks on targets is as extensive as that of constructional technology, but this thesis focuses on a specific sort of attack known as denial-of-service (DoS) attacks. DoS assaults are a form of targeted attack whose purpose is to deplete the target's resources and, as a result, prohibit large customers from obtaining service. For quite some time, great focus has been placed on the Quantum Computing (Security) of network

infrastructure, which has continued to be used for a variety of transactions. The internet Quantum Computing (Security) business, academia, and even the United States Conference, which has organized multiple conferences on the subject, have all taken notice [1, 2]. Various safety strategies have been proposed, each attempting to address a different set of issues. The anonymous attack is the specific risk that this research focuses on. Because the Source Address (SA) information is spooled in the attack packages, the identity of the attacker(s) is not immediately visible to the individual in anonymous attacks.

1.2 Denial-of-Service Attacks

The focus of this thesis is on service denial (DoS) attacks on PC networks. The goal of these attacks is to deny legitimate users access to network services. This PhD includes a comprehensive look at many attack and defence mechanisms, as well as unique defensive mechanisms and new information on defensive mechanism selection and evaluation. DoS mitigation is an important part of network and computer Quantum Computing (Security). Network and computer Quantum Computing (Security) are frequently discussed in scientific domains. Computer Quantum Computing (Security) language is still imbalanced, which is a big issue [10, 11]. Computer and network Quantum Computing (Security) were originally prioritised in the mid-1970s, and some of the most meticulous Quantum Computing (Security) documentation was published in [12]. Denial-of-service attacks come in a variety of forms, and the number of them is expanding all the time as new procedures and data networks are developed. These attacks should be divided into two categories: physical and virtual, with the purpose of better comprehending the most common denial-of-service (DoS) attempts (or network-based). There are two other types of attacks that fall within this category, each of which represents the attack's overall goal: disabling critical services and draining system resources [13].

An Overview of Denial-of-Service Attacks
System disruption (DoS) attacks have been shown to be a significant and long-term threat to users, businesses, and internet infrastructure [16–20]. Blocking access to a specific object, such as a web application, is one of the key targets of these assaults. There have been numerous DoS guards proposed in the literature, but none of them can be trusted with any degree of certainty. Vulnerable hosts on the internet, as well as attack traffic sources,

are virtually certain to be exploited. It's just not possible to keep every host on the internet secure at all times. (In July 2005 it was assessed that there were roughly 350,000 hosts on the internet.) Furthermore, detecting and channelling legitimate traffic attacks without causing legal traffic injury to collateral is quite difficult.

A DoS attack can be carried out in one of two ways: as a flood or as a logical attack. A flood DoS attack is based on brute force. A victim is given as much information as possible, even if it is unneeded. This squandering of network bandwidth fills space with unnecessary data (e.g., spam mail, garbage files, and deliberate error messages), loads flawed data onto fixed-size data structures inside host software, and necessitates a significant amount of data management effort. To increase the impact of DoS attacks, they might continue to be planned from multiple sources (Distributed DoS, DDoS).

1.2.1 DoS Attacks in Real Life

Actual internet DoS instances were investigated throughout the popular era of 1989 to 1995. The three most common consequences were as follows: in 51% of the cases, there was a circle, and in 33% of the cases, there was a network decline of 33%, and in 26% of the cases, certain vital data was deleted. A single occasion can result in a variety of problems (the whole of rates is more than 100%). A college was the target of the first big DDoS attack in August 1999. This attack disabled the target's network for two days. On February 7, 2000, a few key web-based locations were attacked, and they were cut off from the internet for many hours. These DDoS attacks may occasionally cause a single victim's assault movement of around 1 Gbit/s.

The quantity, duration, and location of distributed denial-of-service (DDoS) attacks on the internet were tracked using scatter monitoring. Backscatter is defined as the victim's spontaneous reflex movement in response to the assault package, which is sent with fake IP addresses. In the three weeks of investigation in February 2001, over 12,000 attacks were registered against over 5,000 distinct victims. Packet fragmentation was studied in real networks. Bugs in fragmented management software are exploited in various logic DoS assaults, and the results of this emphasis still suggest the presence of such DoS on the web.

According to the Associated Press, the Emergency Response Team (CERT) Operations Unit was attacked in May 2001. Its portal was down for a few days due to a distributed denial of service (DDoS) attack. In the mid-2002, ISPs in the United Kingdom were focusing on DDoS assaults. Some

clients experienced a 12-hour outage as a result of one of these attacks. The Domain Name System (DNS) continues to put a focus on DoS threats (DNS). In October 2002, all root name servers were subjected to an exceptionally large DoS attack. Because of the damage produced by the assault, certain DNS requests were unable to reach a root name server. On June 15, 2004, a second DoS attack was launched against the Akamai Content Distribution Network (CDN) name servers, preventing access for nearly two hours. The most influential places were Apple Computer, Google, Microsoft, and Yahoo. These companies have outsourced their DNS services to Akamai for service updates.

1.3 Related Work

Denial of service (DoS) attacks have become widely acknowledged as a severe threat to the internet. Threat actors flood a target network with traffic, rendering network services unstable or completely unavailable as a result. It is vital to recognise these assaults in order to prevent them from happening again. To perform this assignment, the exploitability of hidden, simulated, or spoofed exploits must be assessed. In the world of information technology, this is known as an informatics Trace back disadvantage. The use of routers to put self-identifying data into packets travelling down the attack path is how packet marking is done. In PPM routers, packets are labelled with a probability distribution. The amount of tagged packet samples received by a victim node determines its capacity to reconstruct the attack route. We discovered that marked packets from distant routers are highly likely to be noticed by downstream routers when analysing the efficacy of a particular marking chance for all routers in PPM. The overall result will be a drop in the number of packets while there is an increase in the amount of data. By approving each router to regulate the marking chance, a more uniform distribution is achieved. The goal of a dynamic technique is to account for movement while determining the router's position in the attack path. However, many approaches rely on underlying protocols, necessitating the use of routers to manage data on vast networks regarding potential victims. This increases the router's overhead and consumes an excessive amount of time. As can be shown in this study, we have a great desire to propose a method that dynamically sets the value of the marking probability depending on the 8-bit TTL field inside the informatics header, which can be accessed directly by routers without the need for external assistance. We may use the projected TTL worth as a technique of determining where along the attack route the packet is placed and derive

the marking chance value by using the TTL worth as an estimate of the distance covered by a packet. We created a user-friendly computer that imitated the algorithm by simulating it using a variety of test situations. Our dynamic theme, which rebuilds the attack path with more precision while consuming fewer resources at the router and at the target, is successful. The expected theme's main advantages are its simplicity and low router overhead, but a lot of value may be gained by adopting dynamic ways that produce similar outcomes and outperform static approaches across a wide attack range.

1.3.1 Probabilistic Packet Marking (PPM)

New approaches have the potential to increase network overhead, router processing, and node processing. There have been various solutions that have gotten a lot of attention in recent years, including the use of probabilistic packet marking (PPM). Introduce an Associate Degree in this area to expand on the probabilistic packet marking theme, which drastically reduces the number of packets needed to reconstruct the attacker's route.

1.3.1.1 DoS Attacks

Denial-of-service (DoS) attacks may prove to be a serious stumbling block to network connectivity. Some denial-of-service attacks can be avoided if the spoof IP address is reflected back to its original source, allowing the perpetrators to be punished or research into the attack to be done. To fight denial-of-service attacks, IP trace back algorithms are designed to allow for probabilistic packet marking (PPM).

When compared to selected packet marking and electronic messaging schemes—which can be difficult to trace back due to the attacker spoofing the marking field in the packet—Kihong Park *et al.* [1] have planned that probabilistic packet marking—of interest due to its potency and implementation ability—will confer a significant return on investment (ROI) on the victim. Unlike prior study, which found a trade-off between the victim's ability to locate the attacker and the intensity of the DoS attack, which was modelled as a function of the marking chance, route length, and traffic volume, our findings show the inverse relationship: that a low-resource attacker can successfully undertake a distributed denial-of-service attack against a larger target. Minimax problems are the only way to mathematically express this problem. To put it another way, the victim will choose the marking chance, reducing the number of forgeable assault ways available, be focused in a dispersed DoS attack, improving the attacker's capabilities

and reducing PPM's impact. Increasing the marking probability shows that the attacker's ability to disguise his location is limited, but it also shows that the attacker's ability to conceal his position is limited due to sampling limits. Because attackers in normal IP internets would have addresses in two to five equally likely locations, PPM's effectiveness against a single-supply attack is significantly boosted. In a distributed DoS attack, the attacker's uncertainties are concentrated, improving the attacker's capabilities and reducing the effect of PPM.

1.3.1.2 FDPM

According to Yang Xiang *et al.* [2], a unique strategy called flexible deterministic packet marking (FDPM) has been proposed for dealing with large-scale IP trace back assaults, which could be effective in the future in minimising DDoS attacks. During a DDoS assault, the target site or network was continually blasted with fraudulent IP packets from several sources. An IP trace back technique allows you to trace IP packets back to their source (in a somewhat modest manner). FDPM improves packet tracing by offering a number of adjustable options for tracing IP packets, including probabilistic packet marking (PPM) and deterministic packet marking (DPM) (DPM). The FDPM's adaptation choices included the following. It might, for example, increase the length of the marking field in relation to the network protocols currently in use; alternatively, it could decrease the marking rate in relation to the traffic load on the collaborating routers. Because of its use of and display, the FDPM ensures that packet distribution is kept to a minimum in the event of a trace back; for example, it may retrieve up to 110,000 devices from a single incident response. It is possible that even if this page is very heavily loaded, it will still be able to perform a trace back method because of the built-in overload interference mechanism.

1.3.1.3 Simulation Surroundings via Extending ns2

The development of simulation environments and methodologies for measuring the time it takes to trace IP addresses back under a variety of network conditions and malicious attack patterns is critical. A comparison of various PPM (Probabilistic Packet Marking) algorithms is provided, as well as metrics such as the number of packets required to rebuild the attacker route, computational quality, and false positives.

To simulate various PPM approaches, Li *et al.* [3] use an expansion of ns2 along with offensive topology and traffic. The simulation technique can

also be used to test the effects of simulated DDoS attacks on various PPM systems. According to the simulation and analysis results, many of PPM's error-prone elements were in the works, which might help speed up the process of detecting intellectual property infringement.

1.4 Proposed Methodology

Dynamic Probabilistic Packet Marking
Loss of marking information, difficulty reconstructing the attack path, low precision, and other concerns are among the most prevalent repercussions of Probabilistic Packet Marking (PPM). This study utilises a replacement technique (DPPM), which improves the primary prevention method's (PPM) performance even more. Rather than recommending a fixed likelihood of marking, we recommend first determining whether the packet has been marked, and then selecting the most acceptable marking probability from the available possibilities. The adoption of DPPM may be able to resolve the majority of PPM's technical difficulties. DPPM outperforms PPM in the majority of areas, with one exception. As a result of widespread use of public computers and the expansion of network infrastructure, the internet has had a huge impact on modern living, as well as social and economic sectors. Criminal behaviour has become increasingly common, resulting in significant financial losses. The incredibly easy-to-conduct distributed denial-of-service (DDoS) attack has caused havoc on communication infrastructure. Monitoring technology for Internet Protocol (IP) can be used to track the delivery of evidence needed to remedy an assault.

A denial of service (DoS) attack is an attempt to prevent a web-based programme from serving its intended clients, either momentarily by suspending or shutting down the service, or permanently by rendering the application unworkable. A distributed denial-of-service (DDoS) occurs when an attack supply exceeds a single, and in certain cases, multiple information science addresses, as shown in Figure 1.1. In the sense that no customers have come or created disturbances to corporate activities, the front door of a shop or corporation is akin to a gathering of people.

1.4.1 Denial of Service

A denial-of-service (DoS) attack is one that delays or restricts the flow of resources. Denial-of-service attacks can also be triggered by human errors, aesthetic defects, or computer code vulnerabilities. Another example of inappropriate resource utilisation is delays in time-sensitive tasks. During

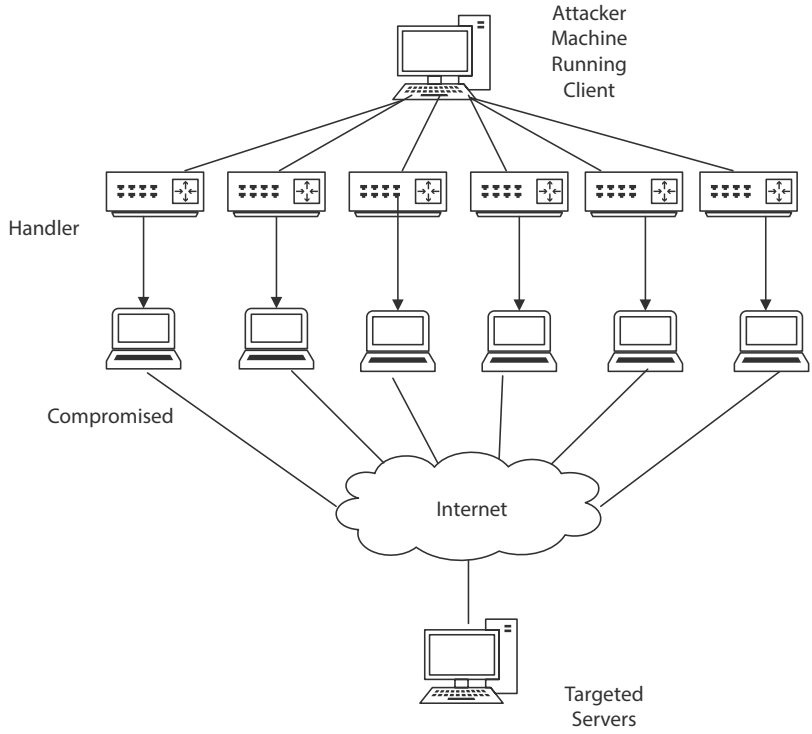

Figure 1.1 DDoS attack.

this defining area, there are samples of resource measurement, process capacity, disc space and memory, and static memory structures. In the ANSI 2000 medium gloss, an attack (that should not succeed) is referred as a Quantum (Security) violation. Since the foundation for a DoS attack has been laid, this can be used.

1.4.1.1 Direct DDoS Attacks

A large number of supply hosts try to prevent victims from consuming resources or deny victims access to resources while attack traffic is sent. An associate degree agent is a hacked server that is used to send attack traffic in connection with a DDoS attack (also known as a daemon, zombie, or bot). A master is an out-of-date group of agents who have been labelled as such. A DDoS network is made up of a collection of linked master agents that are all geared up to help the attacker during DDoS attacks. Direct DDoS assaults and reflector attacks are two types of distributed denial of service (DDoS) attacks.

1.4.1.2 Distributed DDoS Attacks

The attack is frequently delayed as a result of many supply hosts attempting to shut down or tamper with resources given by victims at the same time that assault traffic is being sent. During a DDoS attack, a hijacked host is utilised to transmit attack traffic. A master is a compromised host operation with an out-of-date collection of agents. In the context of a DDoS attack, a DDoS network is defined as a hierarchical collection of linked master agents that helps an attacker organise a DDoS attack with less effort. Reflectors and direct hits are two types of DDoS attacks.

1.4.1.3 Reflector DDoS Attacks

Within the field of supply science, packets containing victims' addresses are supplied to unsuspecting third parties by slave zombies (agents), who successively send a reply to the victim (uninfected computers such as web servers, DNS servers, etc.). (Inundate the victim) a Reflector assault can affect at least two persons. Because of the additional equipment required and the larger bandwidth involved, a reflected assault will be far more devastating. It is also more difficult to keep track of.

1.5 Trace Back Mechanism for Rectified Probabilistic Packet Marking

The internet captures some or all of many crucial and essential services such as banking, commerce, transportation, healthcare, and communication. According to current figures, there are approximately 400 million hosts connected to the internet, and there are currently more than 4 billion internet users. As a result, any network outage could be extremely inconvenient for a large number of individuals. The devastating effects of a DoS attack have drawn the attention of scientists and researchers, resulting in a variety of traumatic processes. The majority of attacks on highly distributed DoS systems that require thousands of compromised PCs, on the other hand, fail. A critical phase in the defence against a Denial-of-Service (DoS) assault is to trace back scientific discipline.

The packet marking technique is used to encrypt the edges data of packets inside routers in a random manner. After that, the victim uses the rehabilitation method to construct the attack path via knowing victimisation. In the past, several traceback procedures in scientific areas were planned. The approach of Probabilistic Packet Marking (PPM) was primarily studied. In

an extremely PPM technique, the router probabilistically stamps the packets with its identifying data, allowing the destination to recreate the network path by combining several packets with similar features. The PPM rule has various issues in the existing system because the termination condition is not explicitly specified. It is necessary to have the necessary configuration information.

1.5.1 A Brief Review of the Packet Marking Procedure

A DoS (Denial-of-Service) attack [4–6], in which a health care helper seeks to build a target host (dubbed a victim) [7, 8] due to the host's large range of packets [9], could be one of the most serious threats to web Quantum Computing [14, 15] (Security). In recent years, DDoS (Distributed Denial-of-Service) attacks have become commonplace anywhere there are many attackers on the internet. From one stage on the Caregiver Path to the next, we set the course of this Associate in the Caregiver Package. IP traceback is a defence mechanism against DoS/DDoS attacks. Every router attacks information about methods to store information about itself or packets in IP traceback systems. The victim then uses the information to track down the offenders. IP traceback systems classify square packet marking (DPM) into two categories: probabilistic (Short PPM) methods and practical packet markings. In PPM protocols, every router almost certainly writes path information on the packets it receives. The IP trace back protocols, on the other hand, generate all collaboration sample packets from routers and store path information on their own. PPM and working methods have a number of benefits. The Figure 1.2 shows about the quantum drones framework.

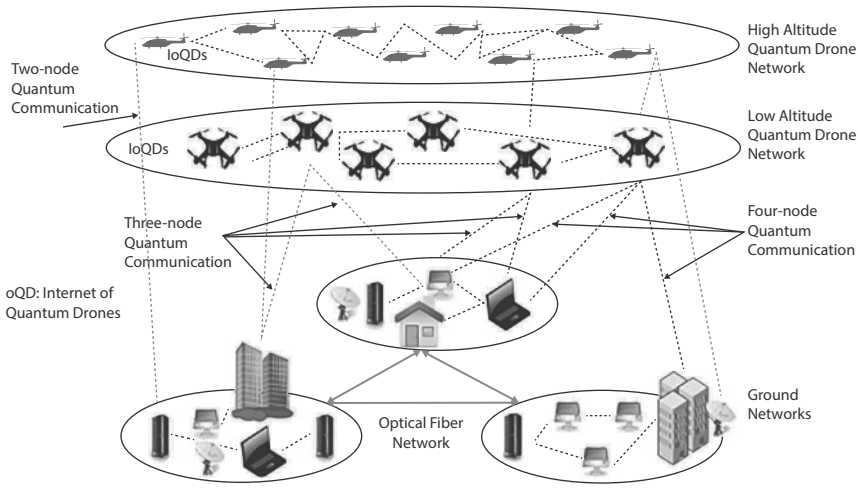

Figure 1.2 Quantum drones.

1.5.2 Packet Marking

PPM does not demand router storage resources, although it typically needs the victim to receive an outsize packet before the attack tree is rebuilt. On the other hand, the quantity of packets for attack tree recovery in work schemes may be low. Work plans nevertheless need considerable load and huge cabinet space on routers. Now, for a current example of traceback information processing protocols let us consider the addition RIHT: a hybrid information processing traceback theme with a p.mark value is computed to find out the packet flow and to look for an attack. This technique takes an outsized amount of calculation into account that requires intense time.

1.5.3 Path Selection

The path describes how the specified packet or file should be delivered from the delivery point to the destination. The upstream interfaces of all routers must be detected and stored in the interface table. The interface table can be used to describe the selected supply and destination.

1.5.4 Packet Sending

In packet or file processing, packet delivery occurs as follows: the packet travels from the source LAN to the destination LAN through the route provided. When the packet is received by the destination LAN, it is checked to see if it has been delivered.

1.5.5 Packet Marking and Logging

On each packet header, a five-bit section is styled as a counter. In our example, if a router decides to sample a packet P with a specific probability, P.counter is set to one, some data is saved on the router, and the packet is finally sent to a neighbouring router. As a result, the higher the counter value, the more routers in the attack path will store P data. In other words, after the attack tree is recovered, a packet with an over-dimensional counter value is favourable. As a result, if we tend to probabilistically prefer a packet with a higher counter worth to a packet with a lower counter worth to a packet with a lower counter worth to a packet with a higher counter worth to a packet with a higher counter worth to a packet with a higher counter.

1.5.6 Path Reconstruction

When employing Formula 3, after the packet reaches its destination, it checks to determine if it was broadcast from the right upstream interfaces. If an assault is detected, the assault will attempt to reconstruct the route. Path reconstruction is the process of discovering a new path for continuous supply and, as a result, a destination that cannot be attacked.

Every significant network attack now includes a DoS or DDoS attack. Although it is relatively easy to die, it may cause significant damage. DoS attacks, which consume a large amount of system resources, render conventional services unusable for genuine consumers. While e-mail has become the most popular mode of communication, DDoS attacks are becoming more common.

Lee and Fung demonstrate how a DoS attack can be carried out utilising an authentication approach based primarily on public-key activity. Many alternative defences against DoS attacks are being considered. Su *et al*. devised an internet strategy based on initial features from estimated sources of associated attack traffic in order to limit the DDoS attack's harm.

Huang *et al*. planned to use associative reward, cooperative filtering, and cooperative caching to help victims of DDoS attacks. As a result, the location of the assault supply would be crucial. Because the supply address is not removed after the router sends a packet to the current protocol, we choose not to accept the supply address in the scientific discipline header of the attack packet.

1.6 Conclusion

A good package marking strategy can cut down on the number of packages needed to trace the victorious path and shorten the time it takes to identify the wrongdoer's genuine supply. There are two sorts of packet marking techniques: static probability marking and dynamic probability theme. We do not always acquire enough tagged packets from faraway routers in PPM, which causes a lot of problems in the IP track and extends the time it takes to reconstruct the victim. Our goal in developing a dynamic probability replacement method was to generate a high enough number of tagged packets from remote routers in a short amount of time in order to perform a faster and more reliable trace back.

References

1. S. E. Cross, "Cyber Quantum Computing (Quantum Computing (Security)," Testimony before the Senate Armed Services Committee, Mar. 2000.
2. R. D. Pethia, "Computer Quantum Computing (Quantum Computing (Security)," Testimony before the Committee on Government Reform, Mar. 2000.
3. S. Gibson, "DRDoS: Distributed reflector denial of service," Gibson Research Corporation," Technical Report, Feb. 2002.
4. Rawat, R. (2023). Logical concept mapping and social media analytics relating to cyber criminal activities for ontology creation. *International Journal of Information Technology*, 15(2), 893-903.
5. Rawat, R., Mahor, V., Álvarez, J. D., & Ch, F. (2023). Cognitive Systems for Dark Web Cyber Delinquent Association Malignant Data Crawling: A Review. *Handbook of Research on War Policies, Strategies, and Cyber Wars*, 45-63.
6. Rawat, R., Chakrawarti, R. K., Vyas, P., Gonzáles, J. L. A., Sikarwar, R., & Bhardwaj, R. (2023). Intelligent Fog Computing Surveillance System for Crime and Vulnerability Identification and Tracing. *International Journal of Information Security and Privacy (IJISP)*, 17(1), 1-25.
7. Rawat, R., Sowjanya, A. M., Patel, S. I., Jaiswal, V., Khan, I., & Balaram, A. (Eds.). (2022). *Using Machine Intelligence: Autonomous Vehicles Volume 1*. John Wiley & Sons.
8. Rawat, R., Bhardwaj, P., Kaur, U., Telang, S., Chouhan, M., & Sankaran, K. S. (2023). *Smart Vehicles for Communication, Volume 2. John Wiley & Sons*.
9. Mahor, V., Bijrothiya, S., Rawat, R., Kumar, A., Garg, B., & Pachlasiya, K. (2023). IoT and Artificial Intelligence Techniques for Public Safety and Security. *Smart Urban Computing Applications*, 111.
10. M. Andrews and J. A. Whittaker, "Computer Quantum Computing (Quantum Computing (Security))," *IEEE Quantum Computing (Security) & Privacy*, vol. 2, no. 5, pp. 68–71, Sept./Oct. 2004.
11. M. Bishop, "What is computer Quantum Computing (Security)," *IEEE Quantum Computing (Security) & Privacy*, vol. 1, no. 1, pp. 67–69, Jan/Feb 2003.
12. M. Bishop, "Early computer Quantum Computing (Quantum Computing (Security)) papers, part 1," 1998. [Online]. Available: http://csrc.nist.gov/publications/history/index.html [accessed Jan. 3, 2006].
13. E. Skoudis. *CounterHack. A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall, Upper Saddle River, NJ, 2002.
14. Mahor, V., Pachlasiya, K., Garg, B., Chouhan, M., Telang, S., & Rawat, R. (2022, June). Mobile Operating System (Android) Vulnerability Analysis Using Machine Learning. In *Proceedings of International Conference on Network Security and Blockchain Technology: ICNSBT 2021* (pp. 159-169). Singapore: Springer Nature Singapore.

15. AusCERT, "2005 Australian computer crime and Quantum Computing (Quantum Computing (Security) survey," Australian Computer Emergency Response Team, Tech. Rep., 2005. [Online]. Available: http://www.auscert.org.au/crimesurvey [accessed Jan. 4, 2006].
16. N. Brownlee, K. C. Claffy, and E. Nemeth, "DNS measurements at a root server," in *Proceedings of the IEEE GlobeCom, San Antonio, USA, Nov. 2001*.
17. CERT Coordination Center, "Results of the Distributed-Systems Intruder Tools Workshop," Nov. 1999.
18. L. Garber, "Denial-of-service attacks rip the Internet," *IEEE Computer*, vol. 33, no. 4, pp. 12–17, Apr. 2000.
19. Mahor, V., Garg, B., Telang, S., Pachlasiya, K., Chouhan, M., & Rawat, R. (2022, June). Cyber Threat Phylogeny Assessment and Vulnerabilities Representation at Thermal Power Station. In *Proceedings of International Conference on Network Security and Blockchain Technology: ICNSBT 2021* (pp. 28-39). Singapore: Springer Nature Singapore.
20. K. J. Houle, G. M. Weaver, N. Long, and R. Thomas, "Trends in denial of service attack technology," CERT Coordination Center, Tech. Rep., Oct. 2001.