Journal of Engineering Science and Technology
Vol. 15, No. 1 (2020) 94 - 107

CERTAIN IMPROVEMENTS TO LOCATION AIDED PACKET MARKING AND DDOS ATTACKS IN INTERNET

SATHEESH N.[1,*], SUDHA D.[2], SUGANTHI D.[3], SUDHAKAR S.[4], DHANARAJ S.[5], SRIRAM V. P.[6], PRIYA V.[7]

[1]Department of CSE, St. Martin's Engineering College, Secunderabad
[2]Research Associate, VIT University, Chennai
[3]Department of CSE, Ramanujar Engineering College, Chennai
[4]Research Supervisor, Anna University, Chennai
[5]Department of Digital and Cyber Forensic Science,
Sree Saraswathi Thyagaraja College, Pollachi
[6]Acharya Bangalore B-School, Bengaluru
[7]Department of CSE, Mahendra Institute of Technology, Namakkal

*Corresponding Author: nsatheesh1983@gmail.com

Abstract

Security is the primary factor considered during any transmission process. While providing the needed service, security maintained during the entire process noticed. Here security indicates the protection given to the components situated in the network physically and terms of the logical operations. The attack is the process of preventing the computer system from providing its valuable service to the user in the network (n/w). DDoS attacks are two significant attacks based on the number of involvement of the computer system. The proposes a novel approach spatial Marking (MRK) technique for the DoS attack by tracing back the IP Address (AddR) of the system involved in the attack process. This proposed method identifies the source of the attack process carried out in the n/w resource using the IP AddR allocated to each of the system based on its location information (INFO). This research study mainly focuses on a mitigation strategy to prevent the DDoS attack. The proposed method of IP Trace Back (TrcBck) uses the location of meta-data for finding out the computer machines and is responsible for the creation of transmission delay. In the future, this work would like to use the PCKT MRK scheme along with the packet (PCKT) filtering to prevent the IP flooding attack in the wireless environment.

Keywords: Attacks, DDoS, Internet Security, IP trcBck, Spatial MRK.

1. Introduction

The internet plays a significant role in communicating to the corners of the world and made the world a smart village. It had created a considerable impact on today's world because of its high degree of availability at less cost. However, it is extremely vulnerable to malicious attacks and threats, which have raised the necessity to identify those attack mechanisms and prevent the Internet from threats. The DDoS is an endeavour to create a computer source engaged to its legitimate end-users. DDoS defence process has two stages. Stage one is to find the origin of an attack. Phase two is to execute the defending mechanism to counteract the attack. Though many solutions have been proposed by both the research experts and commercial communities to counter the DDoS attacks, the problem remains unsolved owing to the connection between the legitimate user traffic and the attack user traffic. N/w security is the process of authenticating the user with a valid login user and a secure code. Once a valid, state-full firewall implements access policies, the type of services is allowed to trusted computer users. IDS services used to identify and prevent malware. An anomaly-based IDS monitor's n/w traffic for suspicious content, unpredicted traffic, and further anomalies to defend the computer n/w.

IP TrcBck is vital for re-establishing in the n/w functions as quickly as likely, avoiding recurrences, and finally, asset the enemies liable. Only detecting the systems that create an attack of n/w traffic might seem like a restricted purpose, but the necessary trace is to present and help to decide the real attacker. Some efforts are less than the approach to improve attacker-detection methods on the Computer Internet. IP TrcBck aims to recognize the practical resource of the PCKTs when the IP AddR is spoofed. There are different categories of TrcBck approaches, including Link testing, classification, messaging, and PCKT MRK. In conventional PCKT MRK, systems require a considerable number of marked PCKTs for each attack and enormous calculation by the victim to identify the basis of the attacks. Therefore, more advanced types of detecting the source of attacking PCKTs are desirable.

In this paper, Section 2 discussed the background works. Section 3 is a proposed Spatial MRK Technique described. Section 4 used to find the Prevention of DDoS Attacks. Section 5 is a result and discussion.

2. Literature Review

Cheng et al. [1] projected a collective detection approach to detect DDoS overflowing attacks over several n/w domains at the traffic-flow level the defence scheme used a Distributed Change-point Detection design CAT and applied over the primary systems operated by ISP. CAT servers cooperate among the methods to mark the result.

ICMP [2] messaging method for IP TrcBck termed as ICMP caddie messages scheme to provide a DoS-impervious result for the n/w related problems. Caddie initiator is an additional ICMP message generated by the PCKT router, which selects the PCKTINFO randomly called ball PCKT forwarded by the upstream router. Ball PCKT used to create the caddie message.

Li et al. [3] proposed a fast binary axioms PPM for the IP TrcBck algorithm, which depends on the part of a self-ruling system, and two types of algorithms are used to rebuild the violent paths. The system reconstructed exactly the attacking

paths between AS based on the number of PCKTs resulting in reducing the data PCKTs required to restore the offensive tracks to the lowest while reducing the complexity of PCKT MRK and rebuilding.

Tan et al. [4] suggested a lively option based PCKTs tracing method by which data PCKTs marked with different source INFO such as Autonomous System and IP AddR. Consider if the temporary PCKT transmitter is both internal/external router, where the former three segments of the IP AddR are patent in case of a stub router selected in the ID and fragment offset field. MRK, the INFO conferring to the correct position of the routers, allows faster and easier path rebuilding.

A reflective statistical MRK system [5] for tracking DoS and DDoS attacks, as well as mirror attacks. The output proved the MRK technique succeeds in an excellent performance in finding the sources of the prospective attack data PCKTs. Besides, it creates minor true positives, whereas other present approaches typically create an assured quantity of untrue positives.

Yang et al. [6] proposed a truncated-level DDoS attack and a high capacity to consume its movement, much like the standard shift. It has the size to avoid the available variance-based finding algorithm. Data metrics are quantifying the differences in n/w transportation using several possibilities of allocations. An innovative metrics like the generalized entropy metric and the INFO distance metric used to find truncated-level DDoS attacks by evaluating the change between authentic traffic and violence traffic positions. The entropy metric discovered attacks multi-hops earlier than the old parameter, and the INFO space metric outperforms the common Kullback–Leibler divergence methodology as it undoubtedly enlarges the decision for space and then achieves the finest discovery thoughtfulness.

An entropy-minimization [7] clustering technique, which divides the attack traffics into bunches, depended on the pooled bottleneck. Consequently, it decreases the mixture of overhead and untrue positives. The method works with TCP/UDP [8] and consumes the INFO at the IP level [9].

These research activities by Padmanabhan and Subramanian [10] in 2001 is the fundamental but critical element that the route from source to destination on the internet, associated with the different studies about geographical location. The concept of TrcBck was pioneered by Burch and Cheswick [11], who concluded the attack route by overflowing complete connections with huge rushes of traffic and computing the alarm in the attack traffic [12, 13]. Song and Perrig [14] in 2000 proposed center track that computerized the traditional idea restoring approach for the path–interference by rerouting attack traffic over expert overlay *n*/*w* design. Stone [15] proposed an improved MRK model for providing TrcBck info in IP PCKTs, which marked the PCKT with a DOMP to make sure that the victim receives all the marked PCKTs with equal probability, which is seriously moderate the number of PCKTs required to rebuild the violent route.

An Advanced MRK Scheme (AMS) [16] presented for the renovation procedure with 2D onset for IP TrcBck. For route recreation attack, the target uses the upstream router diagram as a road-diagram and executes a BFS from the source. Therefore, it diminishes the time of reform and overhead and develops precision.

Liu et al. [17] and Xiang and Zhou [18] offered a new method, called Bendy Deterministic PCKT MRK (BDPM), to execute high-scale IP TrcBck to protect

beside DDoS attacks. The flexibilities of BDPM are in two ways, first is that it adjusts the distance of the MRK arena permitting to the n/w rules arrayed, and the other is that it improves the MRK ratio rendering to a weight of contributing routers.

Jing et al. [19] in 2005 proposed a distributed-log-based IP TrcBck system to defeat DDoS attacks. The practices of PCKT design, proof assembly, and TrcBck handling dispersed among the distinct modules-MRK agent, TrcBck service provider, and an evidence collection agent. Tseng et al. [20] in 2006 proposed an improved system in probabilistic PCKT MRK for IP TrcBckin contradiction of DDoS attack. The proposed ID-based PPM for IP TrcBck is an improvement on the novel PPM's difficulty of fragment mixture over clustering these fragments in the spread, thereby dropping the interval of fragments mixture, the attacking route renovation, and attack reply interval. Based on the idea adopted in the DPM and traditional TrcBck schemes, Gao and Ansari [21] in 2005 proposed a new system, called, Directed Geographical TrcBck (DGT). The concept of ICMP based TrcBck was first proposed by Bellovin et al. [22] in iTrace, which showed sending a small size of ICMP-based out-of-band messaging INFO for the target to sense PCKT review imprints [23, 24].

3. Methods and Materials

3.1. Spatial marking method

Nowadays, a DDoS [25] attack fakes an added threat to a significant number of administrations due to the sum of schemes complicated in retrieving the Internet. It leads to traffic, and INFO access becomes difficult. To overwhelmed these problems, four simple countermeasures besides the attacks viz. finding, justification, avoidance, and TrcBck are required. Furthermost of the researches is supported mostly in the dual ranges viz. attack TrcBck/mitigation. This learning emphases mostly on the TrcBck of IP AddRs recycled for the info communicated and attack route.

3.2. A novel approach for packet marking method

In the PCKT MRK technique, TrcBck data is implanted into the IP PCKT by the routers on the route to the target node. The PCKTs are marked as they traverse routers through the Internet either probabilistically/deterministically. The routers mark the PCKT with either the router's IP AddR or the boundaries of the route that the PCKT navigated to spread the destination/victim and store data in the identification arena of the IP header. The victim uses the routing INFO in the marked PCKTs to trace an attack back to its source. For the main alternative, MRKPCKTs with the router's IP AddR [26], the analysis illustrated that to advance the correct attack lane with 96.16% precision as many as 3,42,000 PCKTs are mandatory. The next method, control MRK, needs that the two nodes that make up a control mark of the path with the IP AddRs along with the distance between them. This approach would require more state INFO in each PCKT than humble node MRK but does faster meet. Types of PCKT MRK are PPM/DPM. The deterministic PCKT MRK approach focuses on determining the source of the attack PCKT and is not concerned with the actual path traversed by the attack PCKT, while the probabilistic PCKT MRK approach emphases on recreating the complete attack route through, which the malevolent PCKTs have navigated. The PCKTMRK method exhibited in Fig. 1.

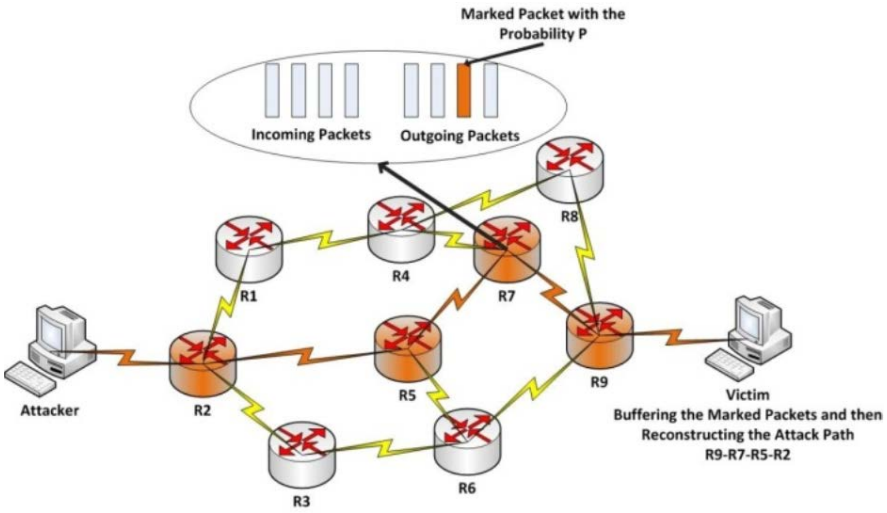

Fig. 1. Packet marking against attacks.

3.3. Directed geographical trcbck and drawback

The directed geographical TrcBck standard involves a track field in the IP header that resides of eight sub-fields that signifies eight potential physical commands. The internet route path span should not exceed more than 32 bits and is essential to encrypt every route [27]. Therefore, 40 bits are mandatory for the entire pa packet route. When a router forwards a PCKT by DGT, it initially agrees with the subsequent hop and then drops the TTL by one and adds 1 to the resultant route subfield. Regardless of the source IP AddR, which is spoofed, the victim has positioned the virtual position of the attacker from the route field when a PCKT attains towards it. If the router has more than eight boundaries and spoofed MRK, then the DCT norm will not work. The drawback of placing the router at the midpoint of the gridline in the DGT technique is very tedious. Since an actual effective TrcBck and attack, a modification tool is essential to overcome the restrictions in the above-cited methodologies. This work proposes a fast convergence IP TrcBck tool named Spatial MRK Technique (SMT).

3.4. Operational standard of SMT

If the PCKT initiates from every machine, its physical info encoded in the IP header when it arrives at the primary router. Physical info code is unknown but more than a bit rate linked with a consistent state. A unique PCKT MRK algorithm in the identification field of the IP header to ensure the location of the arrival of the PCKT in the n/w. It recycled for reuniting fragments. Since the fragmented PCKTs are identical infrequent, the ID field of 16 bits used for storing the INFO. But these 16 bits are not adequate to encode the INFO about all the 13 eras of division process and its quadrant rate. In addition to that, the type of check field of the IP header, which is about 8 bits and a flag bit, is also be used to encode the INFO. So in total, it has 25 bits (16+8+1). The deployment of these bits for keeping the physical position clues to the identification of the location to which the source of attack goes. The INFO is stored based on the order of the subdivision of the physical state.

4. Proposed Prevention of DDoS Attacks

DDoS is a significant threat for authorized users and denies access for other genuine users to web services. A preventive measure is to allocate the resources based on a technique that does the service to get into an uninterrupted manner. The resource hacking and blocking of the users from not getting the service termed as DoS attack and when it involves the number of distributed sources termed as DDoS attacks.

4.1. Escalation: Attack mechanism

The geographical INFO helps to identify the source responsible for the attack using the Area Identification Pointer (AIP). In the present situation, DDoS plays a significant role in consuming n/w resources. Due to this, the process of finding the source becomes difficult. It is recognized with the help of INFO PCKTs and their degree of arrival to the target device. To overcome drawbacks like traffic, latest techniques, and open-source software, four elementary countermeasures beside the attacks viz. finding, justification, avoidance, and TrcBck are measured. These PCKTs broadly categorized into two primary categories, such as the lawful PCKTs from the genuine user and the attack PCKTs from the cause of the attacker. The course of classifying the attack PCKTs agreed with the aid of common sharing is discussed below.

4.2. Traffic analysing methods

Numerous trackback mechanisms proposed to overcome the DDoS attacks and different standards, such as attack verdict. Here the attack is determined, and the incoming traffic throttled using the divide and conquered fashion. In AD/PAD, all the routers along the n/w path from attack source to the victim, which has to take part in the pushback mechanism, which in turn causes severe overhead to the routers.

4.3. Attack detection using standard sharing

Standard sharing is the progression of outcome the possibility of a let-down, unwanted event in a big set of quantity, or the expansion of INFO. In this research, the standard sharing functional used to detect unlawful PCKTs referred by intruders. A trial of *n* amount of PCKTs acquired from the target device, and those PCKTs are verified by the Standard Sharing technique to discover the real intruder who attacked the target machine. All unlawful PCKTs directed over the upstream router are blocked, and lawful PCKTs are certified to extend its endpoint successively.

$$Z = \frac{\overline{X} - \mu}{\sigma / \sqrt{n}} \tag{1}$$

$$\overline{X} = \frac{\sum_{k=0}^{n} x_k}{n} \tag{2}$$

The comparison in Eq. (1) provides the Standard Sharing where *Z* is the standard sharing of trial PCKTs broadcast. Trial PCKTs selected from n amount of PCKTs for investigation for the attack, and the mean of those trial PCKTs at the target established by the comparison in Eq. (2). An arithmetical hypothesis test is a

technique of making results using data, whether from a systematic analysis or an observational review.

4.3.1. Sampling distribution

All possible samples for a given size taken from the population, and for each example, the statistic calculated - the values of the statistic form in the sampling distribution.

4.3.1. Procedure for testing a hypothesis

The following steps are involved in the hypothesis test:

- Frame H_0 and H_1.
- Select the near significance α.
- Calculate the investigation fact Z, by the data offered in the problem.
- Pick out the critical value at α% using Zα.
- Appeal decision: If |Z| < Z α, agree to H_0 at α% near. Then, discard H_0 at α% near.

Consider the situation in which the victim machine receives several PCKTs, which follows a normal distribution. The mean μ of the PCKTs transmitted at the particular time interval is 50.15 lakhs PCKTs. The standard deviation σ is five lakhs PCKTs. To identify the attack flow in the victim, a random of n is 100 trials reserved. For these, the mean of the PCKTs the victim device transmitted and found to be 50.15 lakhs PCKTs. To check whether the PCKT of the group identified has a significant level of rejection, which is 0.015.

Since $Z = 1 < 1.645$, H_0 is Rejected at 5% near impact. Hence, the formulated null hypothesis is wrong. It has to accept the alternate Hypothesis of traffic and attack has occurred in the situation, as illustrated in Fig. 2. Concerning the analysis made, the traffic occurrence confirmed. The next step is to check whether the traffic caused by more number of requests given by the legitimate user or due to the attack PCKTs sent by the intruders - a single proportion test used for accomplishment.

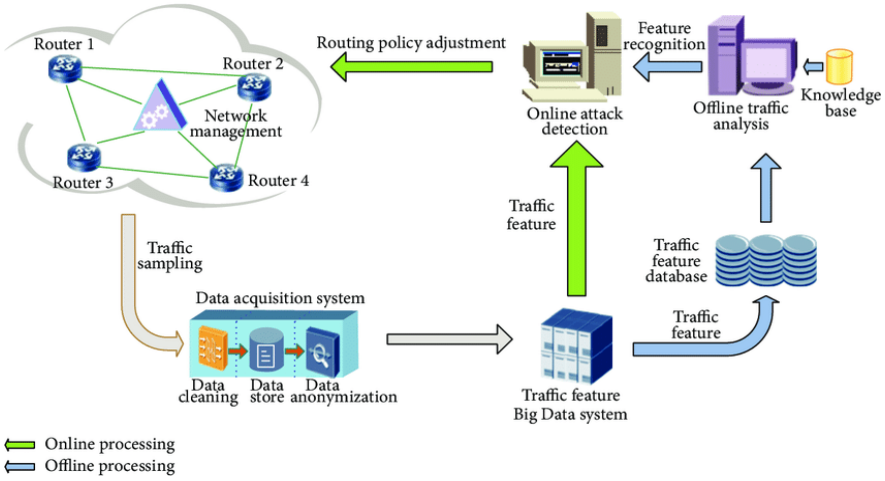

Fig. 2. Attack discovery area.

4.3.2. Distinct unit check

Distinct unit check consumes the INFO about the traffic PCKTs and tests whether the roaming path contains the affected PCKTs. If x is the sum of items owning an individual element is an example of n objects, then the trial section $p = x/n$. Study a trial of size n with unit P taken from a population. Let P be the population unit. To test whether the variance between trial section P and population unit p is primary or not. The trial has been select from the population unit and then proceeds as follows (refer to Fig. 3). Let the unimportant hypothesis be H_0: $p = P$, i.e., p has a fixed rate. The alternative hypothesis is H_1: $p! = P$.

The comparison, Eq. (3), which defines the typical check

$$Z = \frac{P - q}{\sqrt{pq / n}} \tag{3}$$

In a web server, a sample of 100 PCKTs drawn. In that, assume 95 PCKTs attacked PCKTs, and continuing are valid PCKTs. They both attack PCKTs, and valid PCKTs similarly distributed in the specific webserver at 5.13% near impact $Z = \frac{P - q}{\sqrt{pq / n}}$.

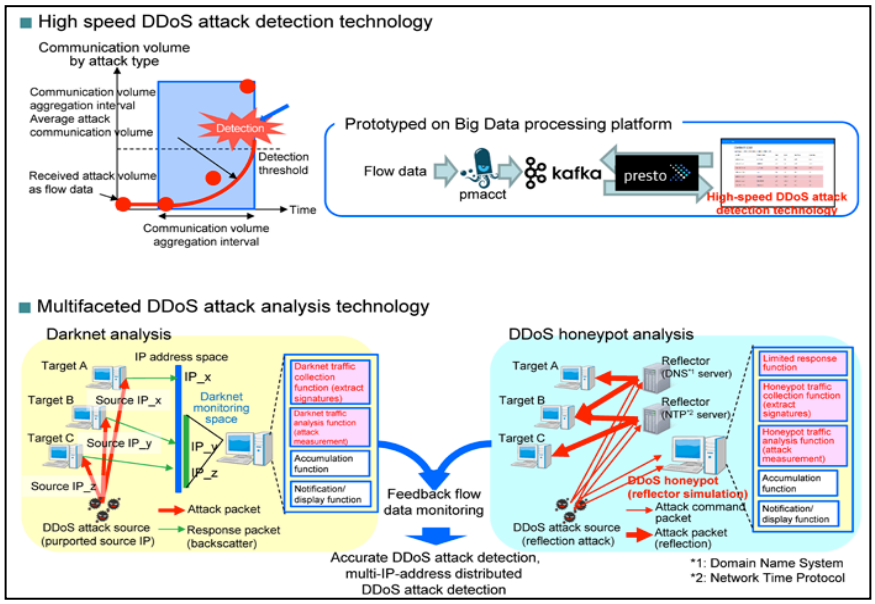

Fig. 3. Attack PCKT detection.

4.4. Role of faith organization helmet (FMH)

FMH is a trivial justification tool to moderate time flooding DDoS attacks, which uses authentic users from attackers. The INFO kept on the users is called a certificate and is given to each user to message, and standard calculation referred. The total number of accesses AN and Inputted Hash (IH) of the concatenation of all the above, with a 128-bit server PIN SP as the key.

4.4.1. Tautological implication theorem

A statement that is true for all possible values of its propositional variables is called a tautology. The reason for selecting at redundancy is, it produces the result outcomes, which is either true/false value. The result based on the condition in which the parameters analysed. Three parameters, namely A, B, and C, in which the tautology process carried out. Then the possible outcomes are as mentioned in Table 1.

The tautology represents the possible valid values as outcomes of the given condition - the result based on the filtration process. The false finding omitted as the sign of discard.

From Table 2, an experimental analysis depends on the number of users present in the group. If the user is accessing the n/w as a single, then based on the browsing history, the Faith Organization (FO) identified. If a group of people in the n/w is accessing the server, then the FO factor is calculated based on the number of trusted requests from the user present in the group. The trusted request varies grounded on the user type and individual faith organization factor. Hence, the FO factor used to identify the genuine user based on the browsing history.

Table 1. A truth chart for repetition.

A	*B*	*C*	**Repetition result** ($A \cup B \cup C$)
0	0	1	Correct
0	1	0	Correct
0	1	1	Correct
1	0	0	Correct
1	0	1	Correct
1	1	0	Correct
1	1	1	Correct

Table 2. Result analysis of the faith organization factor.

No. of users	No. of REQ PCKTs	REQ towards trusted locates	REQ untrusted locates	% of FO factor
05	200000	15000	5000	75.45
10	55000	47000	3000	94.56
50	455000	565000	105000	73.38
100	820000	850000	20000	96.46

4.5. Percolation using redundancy

Tautology defined as a logic statement that is true by necessity/by its logical form. It returns either real value or false value based on the condition used. It helps to monitor the importance of the parameters considered and precede the process. It is the method of promoting the INFO PCKT when all the associated INFO parameters about those PCKTs are accurate. Here, this scheme may check only three settings because it is equal to all the parameters. These three parameters play a significant role in deciding whether the PCKT accepted for processing or rejection. Three vital parameters, such as destination AddR, size of the PCKT, and SMT values. These

parameters are analysed and processed for further PCKT filtration. The SMT value used for identifying the particular region, and along with the additional parameters, the attack PCKTs from the source of the attack blocked. This process helps us to achieve filtration of the efficient attack PCKT. The process involved in the preventing of PCKTs explained below. The tautology applied for the PCKT filtration. Let us consider the parameters as the condition field for the repetition and block the attacked PCKTs. Tautology helps us to recognize the attacked PCKTs and to sieve them efficiently. However, attack PCKTs are found and filtered efficiently. Further analysis of the SMT value gives the location where the PCKTs source is from attacked PCKTs filtered from the source itself.

4.6. Preventing of DDoS attack

For avoiding DDoS attack, the RIM value is used, which obtained by using three parameters such as destination AddR, size of the PCKT, and RIM value. These three parameters are analysed under the tautology method to find the RIM value. The tautology applied for the PCKT filtration. Here the set X refers to RIM values by the victim that is X_1 is destination AddR X_i, X_j, X_k are the given RIM values by the victim that is X_i is destination AddR, X_j is size of the PCKT, and X_k is SMT INFO, the other set P refer to *RIM* values for the PCKT sent by the upstream routers. The upstream router compares these three parameters X_i, X_j, X_k. *If* the packet found, then the router moves those PCKTs into the spam, as mentioned in Table 3.

Table 3. Repetitious tables.

Set PCKT			**Trial PCKT**			**Repetition using NAND GATE**	**Achievement**
x_i	x_j	x_k	y_i	y_j	y_k	$(X_i \uparrow Y_j) \uparrow (X_i \uparrow Y_j) \uparrow (X_i \uparrow Y_j)$	Block/agree
P_i	Q_j	R_k	P_i	Q_j	R_k	0(invalid PCKTs)	Block
P_i	Q_j	R_k	P_i	R_k	Q_j	1(valid PCKTs)	Agree
P_i	Q_j	R_k	R_k	P_i	Q_j	1(valid PCKTs)	Agree
P_i	Q_j	R_k	Q_j	P_i	C_k	1(valid PCKTs)	Agree
P_i	Q_j	R_k	Q_j	R_k	P_i	1(valid PCKTs)	Agree
P_i	Q_j	R_k	R_k	B_j	P_i	1(valid PCKTs)	Agree
P_i	Q_j	R_k	Q_j	Q_j	Q_j	1(valid PCKTs)	Agree
P_i	Q_j	R_k	R_k	R_k	R_k	1(valid PCKTs)	Agree
P_i	Q_j	R_k	P_i	P_i	P_i	1(valid PCKTs)	Agree

5. Result and Discussion

This review supports to analyse the PCKT INFO and sieve it grounded on the accessible INFO. It feeds the INFO in the PCKT only once when it arrives into the primary router in the n/w. The computational weight and scalability association with different methods shown in Fig. 4. Compared to the AD/PAD method, it is preventing meritoriously realized with the support of the SMT method. The FO helmet, along with typical sharing and tautology, shows a foremost part in preventing the attack. It decreases the overhead at the router phase and raises its routine. The trusted user level used for filtering out the attacker from the authorised user.

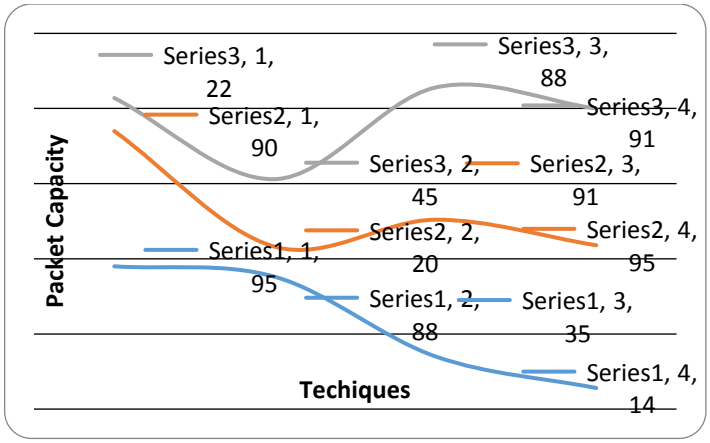

Fig. 4. Performance comparison.

6. Conclusions

A node of the internet is severely affected by the threat imposed by hackers and trespasser. Among the attacks, a DoS/DDoS is essential to tackle the adversary situation caused by it. IP TrcBck system attempts at isolating and identifying the target devices. To make a dynamic IP, TrcBck has presented geographical division with RIM value. By this method, control overhead associated with the upstream router decreased as an intermediate route not distributed in the TrcBck of the IP AddR of attack device. With the help of the tautological implication theorem using typical sharing, mitigation of attack PCKTs done in target devices. The proposed system not confined to a particular location, and then the attack is made through multiple directional and is handled by subsequently attack PCKTs prohibited from traveling further into a target device. In this scenario, directed geographical TrcBck, where the trackback depends mostly on geographic INFO, rather than the IP AddR, which might have spoofed, was proposed. In their basic scheme, an elementary notion of placing the routers at the midpoint of the grid was recommended, limited to a small set of directions.

Also, the thwarting is achieved with the help of SMT INFO value by sending it to the upstream router for efficient filtering, rather than the overhead at the router owing to the pushback mechanism proposed. This work has successfully overcome the dimensional constraints and router fixing at a midpoint of the grid constraints; mainly, the problem occurred in setting up the number of interfaces used in the routers. Now technology has undertaken IPV6 to overcome issues concerned with assigning the IP AddR to an individual node in all directions of the earth. Subsequently, threat and attack imposed by intruders are increasing. In the future, the PCKTMRK scheme, along with the PCKT filtering, is used to prevent the IP flooding attack in the wireless environment, such as the PCKT INFO, which used to the PCKT grounded on the wireless access point INFO.

Nomenclatures

n	Entire number of packets in trial
p.dip	Destination address

p.smt	Physical division traceback information value
p.size	IP size of the packet
$\overline{X}$	Mean of trial packet in the target device
X_k-k^t	Rate of certain trial packet
Z	Standard sharing for packets broadcast in the target device

Greek Symbols

μ	Mean of population packets in target device
σ	Standard deviation of the population

Abbreviations

ADDR	Address
AIP	Area Identification Pointer
AMS	Advanced Marking Scheme
ASN	Autonomous System Number
CAT	Change Aggregation Trees
DCD	Distributed Change-Point Detection
DDoS	Distributed Denial of Service
DGT	Directed Geographical Traceback
DoS	Denial of Service
DPM	Deterministic Packet Marking
FOH	Faith Organization Helmet
FTP	Fast Two Phrases
IDS	Intrusion Detection System
INFO	Information
PCKT	Probabilistic Packet Marking
PCKT MRK	Packet Marking
PPM	Probabilistic Packet Marking
SMT	Spatial Marking Technique
TMH	Trust Management Helmet
TRCBCK	Trace Back

References

1. Cheng, L.; Divakaran, D.M.; Lim, W.Y.; and Thing, V.L.L. (2015). Opportunistic piggyback marking for IP traceback. *IEEE Transactions on Information Forensics and Security*, 11(2), 273-288.
2. Wang, H.; and Shin, K.G. (2003). Transport-aware ip routers: A built-in protection mechanism to counter DDoS attacks. *IEEE-Transactions on Parallel and Distributed Systems*, 14(9), 873-884.
3. Li, Q.; Feng, Q.; Hu, L.; and Ju, J. (2005). Fast two phrases PPM for IP traceback. *Proceedings of the Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT)*. Dalian, China, 386-389.
4. Tan, W.-P.; Lee, B.-S.; and Lee, H.C.J. (2004). Entropy-minimization clustering technique for probabilistic packet marking scheme. *Proceedings of the IEEE International Conference on Networks (ICONS)*. Singapore, 292-295.

5. Xiang, Y.; Lin, Y.; Lei, W.L.; and Huang, S.J. (2004). Detecting DDOS attack based on network self-similarity. *IEEE Proceedings-Communications*, 151(3), 292-295.
6. Yang, X.; Li, K.; and Zhou, W. (2011). Low-rate DDoS attacks detection and trcbck by using new information metrics. *IEEE Transactions on Information Forensics and Security*, 6(2), 426-437.
7. Yu, S.; Zhou, W.; Guo, S.; and Guo, M. (2016). A feasible IP trcbck framework through dynamic deterministic Packet Marking. *IEEE Transactions on Computers*, 65(5), 1418-1427.
8. Gao, Z.; Ansari, N.; and Anantharam, K. (2004). A new marking scheme to defend against distributed denial of service attacks. *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*. Dallas, Texas, United States of America, 2256-2260.
9. Al-Duwairi, B.; and Manimaran, G. (2006). Novel hybrid schemes employing packet marking and logging for IP traceback. *IEEE Transactions on Parallel and Distributed Systems*, 17(5), 403-418.
10. Padmanabhan, V.N.; and Subramanian, L. (2001). An investigation of geographic mapping techniques for internet hosts. *ACM SIGCOMM Computer Communication Review*, 31(4), 173-185.
11. Burch, H.; and Cheswick, B. (2000). Tracing anonymous packets to their approximate source. *Proceeding of the 14th USENIX Conference on System Administration*. Berkeley, California, United States of America, 319-328.
12. Chen, S.; and Chow, R. (2004). A new perspective in defending against DDoS. *Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS)*. Suzhou, China, 5 pages.
13. Sudhakar, S.; and Pandian, S.C. (2016). Hybrid cluster-based geographical routing protocol to mitigate malicious nodes in mobile ad hoc network. *International Journal of Ad Hoc and Ubiquitous Computing*, 21(4), 224-236.
14. Song, D.X.; and Perrig, A. (2001). Advanced and authenticated marking schemes for IP traceback. *Proceedings of the Conference on Computer Communications. Anchorage, Alaska*, United States of America, 9 pages.
15. Stone, R. (2000). CenterTrack: An IP overlay network for tracking DoS floods. *Proceedings of the 9th Conference on USENIX Security Symposium.* Denver, Colorado, 14 pages.
16. Ren, W. (2005). Toward global internet services to defend against DDoS by dynamic possibility-based packets marking trace back. *Proceedings of the International Conference on Services Systems and Services Management. Chongquing, China*, 589-592.
17. Liu, W.; Duan, H.-X.; Wu, J.-P.; and Li, X. (2005). Improved marking model ERPPM tracing back to DDoS attacker. *Proceedings of the Third International Conference on Information Technology and Applications (ICITA).* Sydney, New South Wales, Australia, 759-762.
18. Xiang, Y.; and Zhou, W. (2005). A defense system against DDoS attacks by large-scale IP traceback. *Proceedings of the Third International Conference on Information Technology and Applications (ICITA)*. Sydney, New South Wales, Australia, 431-436.

19. Jing, Y.-N.; Tu, P.; Wang, X.-P.; and Zhang, G.-D. (2005). Distributed-log-based scheme for IP traceback. *Proceedings of the Fifth International Conference on Computer and Information Technology (CIT). Shanghai, China,* 711-715.
20. Tseng, Y.-K.; Lu, Y.-Y.; Huang, J.-Y.; Hsieh, W.-S.; Chang, B.-R.; Chen-Yu, C.; and Chen, S.-H. (2006). ID-Based PPM for IP traceback. *Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC). Beijing, China,* 262-265.
21. Gao, Z.; and Ansari, N. (2005). Directed geographical traceback. *Proceedings of* the *3rd International Conference on Information Technology: Research and Education. Hsinchu, Taiwan*, 221-224.
22. Bellovin, S.M.; Leech, M.; and Taylor, T. (2003). *ICMP traceback messages*. Fremont, California, United States of America: Internet Engineering Task Force.
23. Yang, X.-Q.; Pei, C.; Zhu, C.; and Li, Y. (2005). AMS based reconstruction algorithm with two-dimensional threshold for IP traceback. *Proceedings of the Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT)*. Dalian, China, 781-783.
24. Yu, J.; Fang, C.; Lu, L.; and Li, Z. (2010). Mitigating the application layer distributed denial of service attacks via effective trust management. *IET Communications,* 4(16), 1952-1962.
25. Kao, D.-Y.; Wu, W.-Y.; Su, C.-W.; and Wang, T.-C. (2018). Strategy for detecting IP address of LINE VOIP network packets by using the decision-tree approach. *Proceedings of the IEEE Conference on Application, Information and Network Security (AINS).* Langkawi, Malaysia, 111-116.
26. Saxena, P.; and Sharma, S.K. (2017). Analysis of network traffic by using packet sniffing tool: Wireshark. *International Journal of Advance Research Ideas and Innovations in Technology*, 3(6), 804-808.
27. Sengan, S; and Pandian, S.C. (2013). Trustworthy position-based routing to mitigate against the malicious attacks to signifies secured data packet using geographic routing protocol in MANET. *WSEAS Transactions on Communications,* 12(11), 584-603.