Development of Internet Protocol Traceback Scheme for Detection of Denial-of-Service Attack

O. W. Salami[1*], I. J. Umoh[2], E. A. Adedokun[2]

[1] CAAS-DAC, Ahmadu Bello University, Zaria, Nigeria.
[2]Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria.

ABSTRACT: ABSTRACT: To mitigate the challenges that Flash Event (FE) poses to IP-Traceback techniques, this paper presents an IP Traceback scheme for detecting the source of a DoS attack based on Shark Smell Optimization Algorithm (SSOA). The developed model uses a discrimination policy with the hop-by-hop search. Random network topologies were generated using the WaxMan model in NS2 for different simulations of DoS attacks. Discrimination policies used by SSOA-DoSTBK for the attack source detection in each case were set up based on the properties of the detected attack packets. SSOA-DoSTBK was compared with a number of IP Traceback schemes for DoS attack source detection in terms of their ability to discriminate FE traffics from attack traffics and the detection of the source of Spoofed IP attack packets. SSOA-DoSTBK IP traceback scheme outperformed ACS-IPTBK that it was benchmarked with by 31.8%, 32.06%, and 28.45% lower FER for DoS only, DoS with FE, and spoofed DoS with FE tests respectively, and 4.76%, 11.6%, and 5.2% higher performance in attack path detection for DoS only, DoS with FE, and Spoofed DoS with FE tests, respectively. However, ACS-IPTBK was faster than SSOA-DoSTBK by 0.4%, 0.78%, and 1.2% for DoS only, DoS with FE, and spoofed DoS with FE tests, respectively.

KEYWORDS: *DoS* Attacks Detection, Denial-of-Service, Internet Protocol, IP Traceback, Flash Event, Optimization Algorithm.

[Received May 23, 2018; Revised January 03, 2019; Accepted March 15, 2019] Print ISSN: 0189-9546 | Online ISSN: 2437-2110

I. INTRODUCTION

Security focus includes preventing a security breach before it occurs, (Tamana & Bhandari, 2014), detecting a breach if it occurred and taking remedial actions, and identifying the cause of a breach when it is detected, (Shi, 2017). When prevention fails then rectification of the damages and the search for its cause become necessary. Among network forensic methods often employed to determine the source of a cyberattack is the Internet Protocol (IP) traceback technique, (Deepthi & Arun, 2017). Different IP traceback schemes are available but their applications for tracing different cybercrime incidence is limited, (Patil & Devane, 2017). Denial of service (DoS) attack is a type of cybercrime that requires an IP traceback scheme that can discriminate it from normal network flows that transmit large data in a manner symptomatically comparable to DoS, (Bhandari et al., 2016).

A DoS attacks like Ping of Death (PoD), (Malik & Singh, 2015), or smurf attack, (Schmitz, 2013), disrupts the services of the attacked system by flooding it with tremendous data in order to prevent legitimate access to the services, (Gunasekhar et al., 2014). DoS is not used for stealing, eavesdropping, bridge privacy or to compromise data integrity on a system but to disrupt services.

PoD attack is used to flood the victim with oversized packets. Packets larger than the 65,536 bytes (maximum allowable size by IP Protocol) are sent in fragments. Reconstructing the packet from the fragments will lead to memory overflow (Mary & Begum, 2017). Attackers would usually use spoofed source IP addresses making it difficult to trace its genuine source (Gunasekhar et al., 2014). PoD can simply be executed as distributed DoS (DDoS) attack by spoofing the sender address of the ping packet to be the victim's address. On sending the ping to the network broadcast address, all the systems that receive the request will reply to the victim and exhaust its memory, (Gorla et al., 2015). The attacker only sends fewer attack packets with multiple effects that may be corresponding to the number of nodes that received the ping broadcast and send the echo reply to the victim.

The task of improving IP traceback technique to be able to detect the source of a cyber-attack accurately is a continuous work because IP protocol does not directly support traceback, (Nur & Tozal, 2018). The time required to receive an adequate number of packets needed for reconstructing the attack path is considerably large. Thus, hindering the efficient performance of traceback schemes. Saurabh & Sairam, (2013) used a completion condition method to improve Probabilistic Packet Marking (PPM)'s reconstruction time. Deterministic packet marking (DPM) schemes have a scalability problem. Mark on demand (MOD) was used by (Yu et al., 2016) to mitigate the scalability problem of DPM.

Flash event (FE) is caused by many legitimate users accessing the same service on a server at the same time. This may result in large traffic that can resemble a DoS attack. The traffic surge in a network caused by the flash event may be occurring repeatedly at a time of an event or suddenly at a specific time. An example of such repeated occurrence may happen if a network operator offers free browsing to its user for a limited period at a particular time of the day. It is most likely that there will be heavy traffic on the operator's network at that free browsing period. Election periods also increase

*Corresponding author: salamiow@gmail.com ***doi:*** http://dx.doi.org/10.4314/njtd.v16i4.3

network traffic during voting when unconfirmed results are circulated and when the authentic results are being announced. The surge due to a flash event can occur suddenly due to breaking news announcing a very important incidence, like the death of a president or a famous personality. Those situations described can bring large users online to access the information.

Irrespective of whether the surge brings the network down or not, a flow-based Internet Protocol (IP) traceback scheme that detects attack traffic based on the amount of routing packets only will falsely accept edges in such network with flash event traffic surges as segments of attack path. The described cases are sources of false alarms in existing flow-based IP traceback techniques used for detecting the source of a DoS attack. Kandula, et al., (2005), cited examples of different DDoS attacks crafted to mimic flash event. They called them CyberSlam attacks. CyberSlam attacks may not be traced correctly by IP traceback that does not have a special feature to differentiate different flooding traffics. It will make attacks source detectors that cannot differentiate a flash event surge from the DoS attack traffic to return wrong attack path.

Nature-inspired algorithms are now used to solve complex computing problems, (Osman & Laporte, 1996). Nature-inspired algorithms have superior performance in handling highly complex nonlinear models. Its significant advantages include the ability to combine the natural randomness in data pattern and rules to efficiently detect optimum solutions, (Prayogo et al., 2017). To mitigate the challenges that FE poses to IP-Traceback techniques, this work proposes an IP Traceback scheme for detecting the source of a DoS attack based on Shark Smell Optimization Algorithm (SSOA) called the SSOA-DoSTBK. The SSOA is used in the scheme for implementing a discernment policy to avoid false acceptance of the wrong path by ascertaining the nodes involved in retransmission of the attack packets during a hop-by-hop search.

II. RELATED WORKS

Artificial bee colony (ABC) was used to apply traffic flow information as a feature to find the attack route by Hamedi-Hamzehkolaie et al., (2014). The intensive traffic flows of the attack packets are considered as the food resource the bees are exploring. The most probable attack path is considered to be the path explored by most bees based on the amount of nectar and closeness to the hive. The bees follow the traffic flow to reach a router. This makes the router with more DoS attack traffic flows to be selected. Simulated Rain Drop (SRD) was used by Bhagat & Pasupuleti, (2015) to develop a relay mechanism as a solution to mitigate distributed DoS in cloud computing. SRD is a swarm algorithm and it is used to cover the large area of Cloud computing. When a bottleneck is caused by a DoS attack in cloud computing, the SRD relay mechanism will search for the highest available throughput where data can be rerouted to avoid congested edges affected by the DoS attack.

This solution only finds an alternative route for data rerouting in the presence of a DoS attack. Attack source detection was not the focus of the paper. Nature inspired algorithm based on modified Ant Colony System algorithm called ACS-IPTBK (Wang et al., 2016), has been used for an IP traceback scheme that can detect attack path with a minimum number of packets and without necessarily having complete network routing information. Each ant traverses an attack path. In addition to the global rule of the original ant colony optimization (ACO) used for ant evolution, ACS-IPTBK adds a local rule for a deeper search. The ants drop pheromones on the path as they traverse it. The path traversed by the highest number of ants, which is the path with the highest amount of pheromones, is returned as the most probable attack path.

An IP traceback mechanism using particle swarm system was proposed by Venkataramanan & Ravi, (2017). Particle swarm system is an enhanced Particle Swarm Optimization (PSO) algorithm with a local updating rule in addition to the global updating rule of the original PSO. The incorporated local updating rule is used to enhance PSO efficiency and avoid being trapped in local suboptimal solution, giving better results. This technique was able to reconstruct the attack path using fewer packets than needed by similar previous schemes and was able to trace the source of spoofed attack packets. Saini et al., (2017) developed a hybrid IP traceback mechanism using two nature-inspired optimization algorithms, namely, Ant Colony Optimization and Particle Swarm Optimization.

The two optimization algorithms are swarm algorithms and known to be effective in solving combinatorial optimization problems. The PSO was used to improve the convergence rate and reduce the computational complexity of the ACO algorithm. Because ACO normally performs search operation on the basis of distance it is combined with velocity based PSO algorithm so that premature convergence can be avoided and faster convergence with lesser number of ants can be achieved. Thus, the scheme combined the distance metric from ACO with the direction and velocity metric from PSO to compute probability metric for the IP traceback process. The objective was to improve the traceback time and reduce the number of packets required by IP traceback. The scheme was able to find a more globally optimum solution for IP Traceback problem with improved convergence rate using fewer numbers of ant and particle agents.

There are other solutions that did not employ a nature-inspired algorithm. They include a dynamic deterministic packet marking (DDPM) proposed by Yu et al., (2016), using the mark on demand (MOD) approach to make DDPM scalable and ease its implementation. Another one is Extended Entropy Metric (EEM) for DDoS flooding attack detection and IP traceback, called E-LDAT proposed by Bhuyan et al. (2016). They calculated EEM for each distribution of source IP addresses and compared the calculated EEM values against a threshold value set for the distributions to determine the occurrence of attack after which NetFlow is then used to trace its source.

The existing solutions for DoS attack source detection that employ nature-inspired algorithms use swarm algorithm agents for flow-based detection. However, these techniques do

not consider the flash event that can cause a sudden surge in legitimate traffic flow in different segments of the network.

III. METHOD AND MATERIALS

SSOA-DoSTBK simulation was developed in NS2. Ping and messaging agents were set up using OTCL classes. Messaging is used for generating normal network transaction between other nodes. While the Ping agent is used to generate the ping of death attack by a randomly selected attacker on a randomly selected victim. Other communication protocols or agents including TCP, FTP, CBR are implemented for different other network transactions occurring concurrently on the network.

The network consisted of 25 autonomous systems with 8 nodes each was defined using the TCL code. The topology used for the simulation was generated in the simulator using a random topology simulator written in TCL language of the NS2. The random topology simulator placed the 200 nodes at random coordinate points in the network area. The WaxMan's connectedness probability, *p*, is used to establish connection links attributes which include transmission rates and bandwidth between nodes based on their distance apart.

$$p(i,j) = \eta . e^{\left(\frac{d(i,j)}{L\gamma}\right)} \quad (1)$$

In eqn (1), *d*(*i*,*j*), is the distance apart between the nodes, L is the longest possible distance between any two nodes, η and γ are constant fitting parameters, i and j are the relative coordinates of neighbouring nodes. The values of η were iterated from the sequence [0.3, 0.6, 0.9, 1.2, 1.5] for different generations of the simulation. The value γ = 0.1 was used for all simulations.

Parameters given in Table 1 are unique to the attack packets. They can be used to identify the packets flow on ingress upstream routers. They are extracted and stored in x_0 with their corresponding assigned weights. In the first column of Table 1 are the parameters that can be found on real-life routers, e.g. Cisco routers flow records, (Cisco.com 2009). The second column contains their equivalent in NS2 that were used for the simulation.

Table 1: Weight values assigned to discrimination parameters.

Parameter	NS2 Parameter	Value
ICMP	Pkt_Type	4
IP-ID	Pkt_Id	5
Packet-Length	Pkt_sz	1
Dst IP address	Dst_Node_Id	4
Pkts	Packets_Count	NV
Active	Host_log_Time	1
NextHop	Next_hop_node	2

NV = No Value

The parameter that has the highest value of 5 is the parameter that uniquely identifies the flow. The parameters *packet type* and *destination address* must be the same for all packets of the flow, though they are not unique to the flow, they were assigned 4. The weighting value of 2 is assigned to *Dst Port Msk AS* and *NextHop address* because many other packets forwarded by the same hop will have the same value. The *NextHop address* can only change for packet routed after the routing table of the hop has changed. The parameters assigned a weight value 1 are the ones that can be changed by the attacker such as *MAC address* and the *Packet length*. Server active time is assigned weight value 1 because it does not tell much about the attack route. The number of packets forwarded by the hop within the time frame is not assigned value because it includes other packets that are not attack packets. It is used only to estimate traffic on the hop within the time frame.

The IP traceback scheme proposed in this paper examines the flow traffics on each hop by focusing on those traffics that have the IP address of the attacked system as their destination address. The parameters with weight values 5 are the parameters first searched. The amount of attack packets forwarded by each neighbouring node j is estimated as follows;

$$\chi_e = \sum_{k=1}^{K} (x_{e,k} \cap x_0) \quad (2)$$

The header parameters of each packet, *k*, that was transmitted from a neighbouring node, *j*, connected by an edge, *e*, is denoted as $x_{e,k}$. Every $x_{e,k}$ were examined against the discrimination policy, x_0, up to the total packets, *K*, using eqn (2). The total weights of matching parameters estimated for each neighbouring node is store in χ_e in eqn (2). A sample of attack path reconstruction is shown in Figure 1. The returned attack path from the victim to the attacker consists of the yellow edges. The attacked node is the one that is dropping packets in the figure.

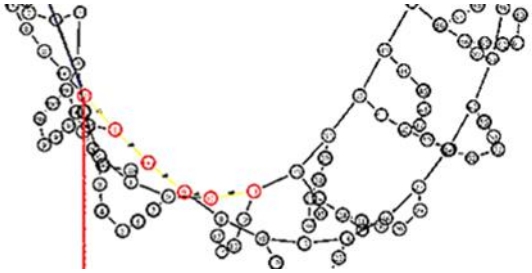


Figure 1: Attack path reconstruction.

A. Performance Evaluation

The performance of the developed scheme was compared against the performance of ACS-IPTK. Performance of the scheme was estimated based on the correctness of the returned path when the simulated attacks were traced back to the attacker under different conditions.

The average attack packet on path returned by the scheme in consideration was indicated as atkPktAve. The total packets routed on the returned path within the time frame in focus was represented as pktTot. The percentage correctness of the path, Peff, was calculated as

$$\text{Peff} = \frac{atkPktAve}{pktTot} \times 100\% \quad (3)$$

In eqn (3), Peff indicates the accuracy of the returned path in terms of the number of attack packets found on the path. The

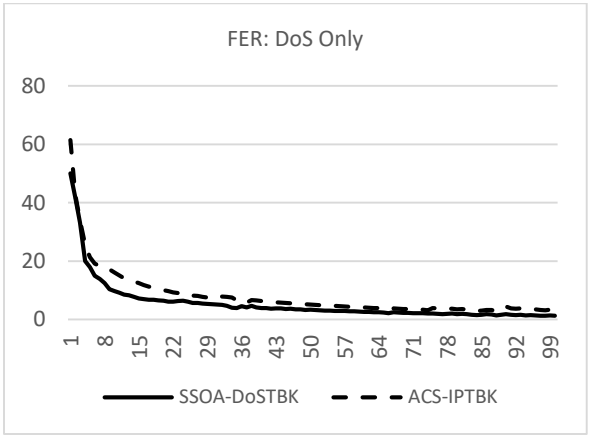
difference between the percentage average performance of SSOA-DoSTBK and ACS-IPTBK indicated as

$$\text{PDiff}(\%) = \frac{S_{AVE} - A_{AVE}}{A_{AVE}} \times 100\% \quad (4)$$

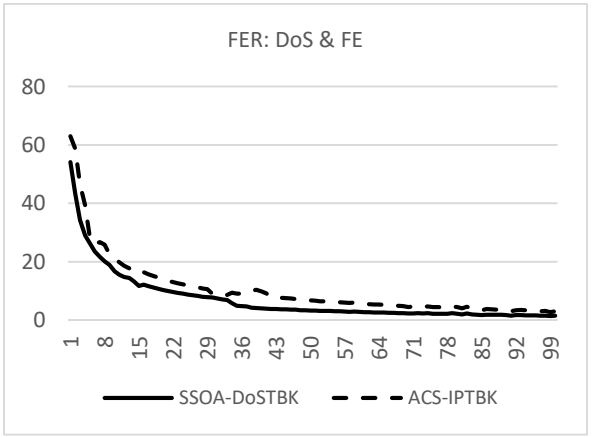
where S_{AVE} and A_{AVE} are the average results obtained for SSOA-DoSTBK and ACS-IPTBK, respectively, in a test. PDiff in eqn (4) is the estimated percentage improvement of SSOA-DoSTBK over ACS-IPTBK.

IV. RESULTS AND DISCUSSION

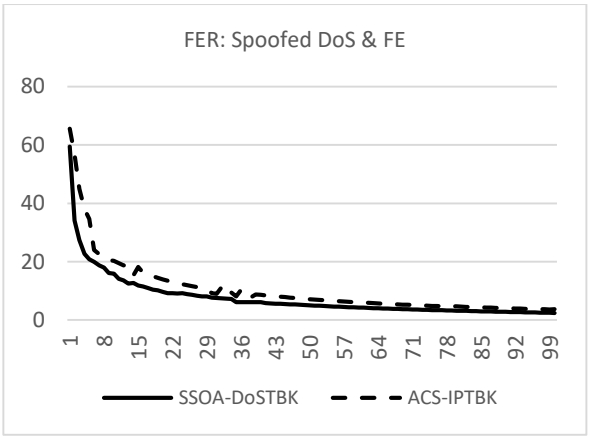
The proposed IP traceback scheme for the source of DoS attack detection was tested on False Error Rate (FER), the accuracy of the attack path returned, and the convergence time. The three tests were performed at three different conditions; first, when only DoS attack is generating traffic in the network, second, when FE and DoS attack traffics are present, and third, when spoofed DoS attack with FE traffics occur together in the network. The results were compared with ACS-IPTBK model. Figure 2 shows the relative performances of the proposed scheme and the benchmark in FER tests.



(a) FER for SSOA-DoSTBK and ACS-IPTBK for DoS only.



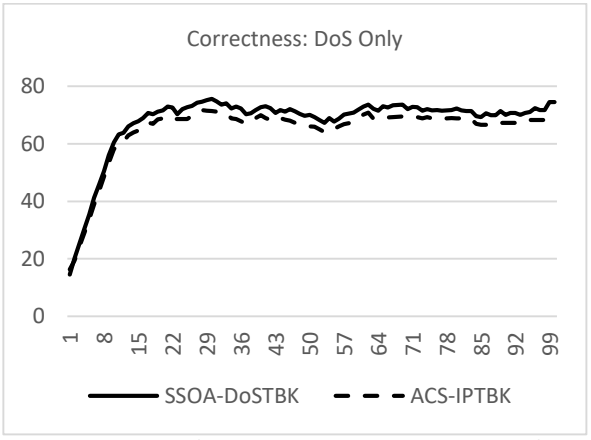
(b) FER for SSOA-DoSTBK and ACS-IPTBK for DoS and FE.



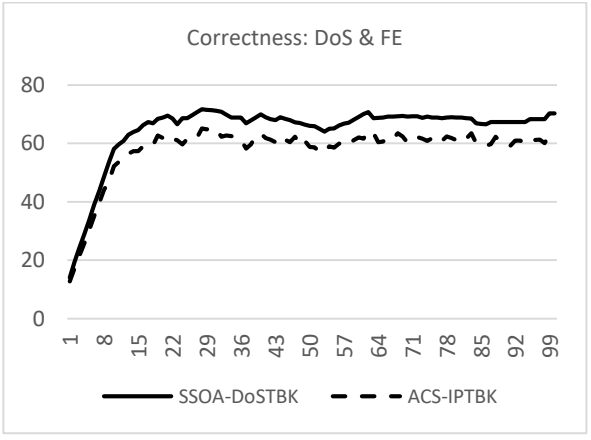
(c) FER for SSOA-DoSTBK and ACS-IPTBK for Spoofed DoS and FE.

Figure 2: Relative FER of SSOA-DoSTBK and ACS-IPTBK.

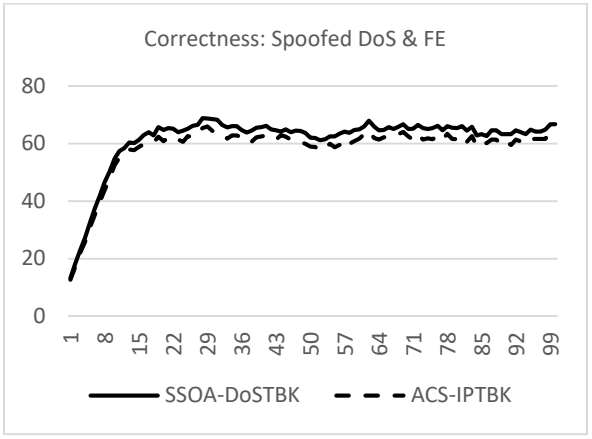
The results of the tests for the correctness of the path returned in terms of the number of attack packets on the returned path are shown in Figure 3.



(a) The correctness of the paths returned in the presence of DoS only.



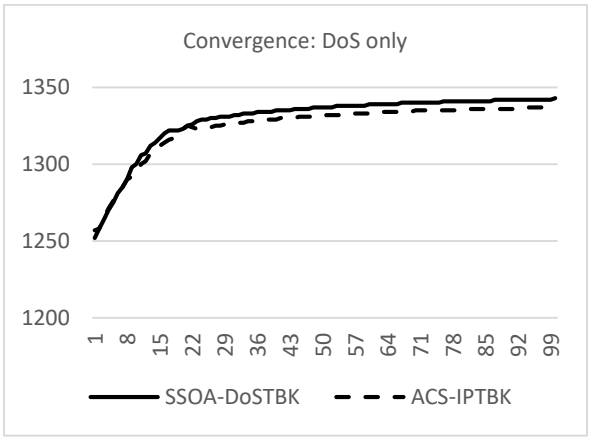
(b) The correctness of the paths returned in the presence of DoS and FE.



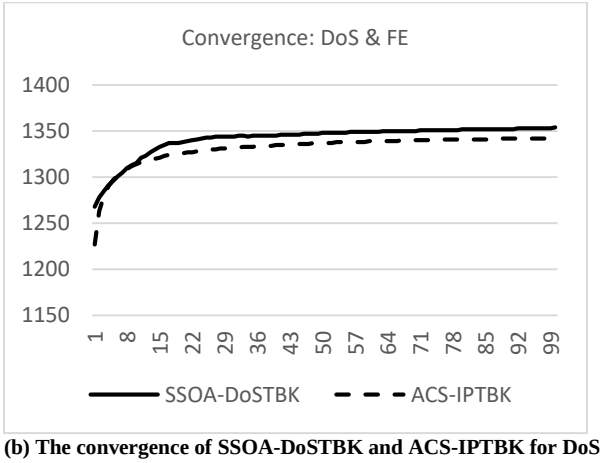
(c) The correctness of the paths returned in the presence of Spoofed DoS and FE.

Figure 3: Relative Correctness of SSOA-DoSTBK and ACS-IPTBK.

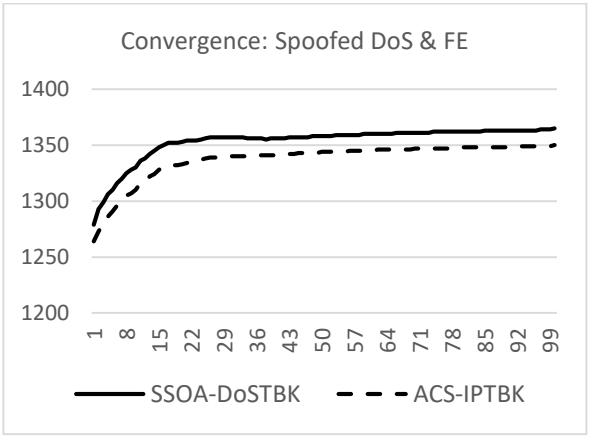
Figure 4 illustrates the convergence of SSOA-DoSTBK compared to ACS-IPTBK. ACS-IPTBK converged slightly faster than the proposed scheme in the tests.



(a) Convergence of SSOA-DoSTBK and ACS-IPTBK for DoS only.



(b) The convergence of SSOA-DoSTBK and ACS-IPTBK for DoS and FE.



(c) The convergence of SSOA-DoSTBK and ACS-IPTBK for spoofed DoS and FE.

Figure 4): Relative convergence of SSOA-DoSTBK and ACS-IPTBK.

B. Comparison of the Quantified Results

The comparison is used to evaluate the functionality and efficiency of the SSOA-DoSTBK over ACS-IPTBK. The quantified comparison values in Table 2 shows that the proposed scheme outperformed ACS-IPTBK in FER and Performance tests by, at least 5.2% in the worst condition and as much as over 32% in the least challenging condition. It also compared favourably with ACS-IPTBK in terms of convergence time by recording a convergence time with a negligible difference compared to the time recorded by ACS-IPTBK as seen in Table 2.

Table 2: SSOA-DoSTBK Convergence compared with ACS-IPTBK.

Tests		Improvement (%)
FER	DoS	31.8
	DoS+FE	32.06
	Spoofed DoS+FE	28.45
Performance	DoS	4.76
	DoS+FE	11.6
	Spoofed DoS+FE	5.2
Convergence	DoS	-0.4
	DoS+FE	-0.78
	Spoofed DoS+FE	-1.2

V. CONCLUSION

Deep search for attack flow was implemented on ingress hops using discrimination policy developed based on details extracted from the attack packets. The discrimination policy was used in a hop-by-hop search to determine the most probable hops involved in forwarding the attack packets from the attacker to the victim. This was aimed at reducing errors in the attack path reconstruction that may cause failure to detect the attack source.

The proposed scheme was implemented in the NS2 version known as ns2-allinone-2.35. It was used for attack path reconstruction under different conditions with ordinary DoS attack alone, when DoS attack and flash event surges were present on the traced path, and when DoS attack with spoofed

packets was present together with FE surge traffic on the attack path. The performance of the developed scheme was measured based on false error rate, the number of attack packets on the returned path, and convergence time. The developed scheme recorded 31.8%, 32.06%, and 28.45% lower false error rate for DoS only, DoS with FE, and spoofed DoS with FE tests, respectively.

It also recorded better efficiency in terms of the correctness of the attack path returned by 4.76%, 11.6%, and 5.2% higher performance in attack path detection for DoS only, DoS with FE, and spoofed DoS with FE tests, respectively. But the ACS-IPTBK was faster than SSOA-DoSTBK in the attack path reconstruction by 0.4%, 0.78, and 1.2% for DoS only, DoS with FE, and spoofed DoS with FE tests, respectively.

The test results show that ACS-IPTBK deviated further than SSOA-DoSTBK from the true attack path. SSOA-DoSTBK is also more effective for detecting the source of spoofed IP attacks. The time difference between SSOA-DoSTBK and ACS-IPTBK convergence was negligibly small. The ACS-IPTBK operates on the basis of parallelism whereby different agents examined different segments of the network concurrently, but SSOA-DoSTBK operates a hill-climbing search. ACS-IPTBK examined more areas most of which are not on attack path but SSOA-DoSTBK narrowed its search to the relevant area based on defined heuristics.

REFERENCES

Bhagat, S. and Pasupuleti, S. K. (2015). Simulated Raindrop Algorithm to Mitigate DDoS Attacks in Cloud Computing. Paper presented at the Sixth International Conference on Computer and Communication Technology 2015, Allahabad, India, 412-418, USA: ACM.

Bhandari, A.; A. L. Sangal and K. Kumar. (2016). Characterizing flash events and distributed denial-of-service attacks: an empirical investigation. Security and Communication Networks, 9(13): 2222-2239.

Bhuyan, M. H.; D. Bhattacharyya and J. Kalita. (2016). E-LDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric. Security and Communication Networks, 9(16): 3251-3270.

Deepthi, S. and Arun, P. S. (2017). A Survey on IP Traceback Techniques. International Research Journal of Engineering and Technology, 4(10): 1643- 1644.

Gorla, M. C.; V. M. Kamaraju and E. K. Çetinkaya. (2015). Network Attack Experimentation using OpenFlow-enabled GENI Testbed. Available online at: https://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=2757&context=ele_comeng_facwork Accessed on May 23, 2017.

Gunasekhar, T.; R. K. Thirupathi, P. Saikiran and P. V. S. Lakshmi. (2014). A Survey on Denial of Service Attacks. Paper presented at the International Journal of Computer Science and Information Technologies, 5(2): 2373-2376.

Hamedi-Hamzehkolaie, M.; R. Sanei, C. Chen, X. Tian and M. K. Nezhad. (2014). Bee-based IP traceback. Paper presented at the 2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Xiamen, China, 968-972.

Kandula, S.; D. Katabi, M. Jacob and A. Berger. (2005). Botz4Sale: Surviving Organized DDoS Attacks That Mimic Flash Crowds. Paper presented at the 2nd Symposium on Networked Systems Design & Implementation, USA, 287-300.

Mary, D. S. N. and Begum, A. T. (2017). An Algorithm for Moderating DoS Attack in Web Based Application. Paper presented at the Technical Advancements in Computers and Communications (ICTACC), 2017 International Conference, Melmaurvathur, India, 26-31.

Nur, A. Y. and Tozal, M. E. (2018). Record route IP traceback: Combating DoS attacks and the variants. Computers & Security, 72: 13-25.

Osman, I. H. and Laporte, G. (1996). Metaheuristics: A bibliography. Annals of Operational Research, 63: 513-628.

Patil, R. Y. and Devane, S. R. (2017). Unmasking of source identity, a step beyond in cyber forensic. Paper presented at the Proceedings of the 10th International Conference on Security of Information and Networks, Jaipur, India, 157-164.

Prayogo, D.; M. Cheng and H. Prayogo. (2017). A Novel Implementation of Nature-inspired Optimization for Civil Engineering: A Comparative Study of Symbiotic Organisms Search. Civil Engineering Dimension, 19(1): 36-43.

Saini, A.; C. Ramakrishna and K. Sachin. (2017). A Hybrid Approach to Address IP Traceback Problem using Nature Inspired Algorithm. Paper presented at the First International Conference on Information Technology, Communications and Computing, Bhopal, India, DOI: 10.5281/zenodo.1130621