International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 9 • Issue 2 pp. 19-27 March 2018 - Sept 2018 www.csjournals.com

Defense against SYN Flooding Attacks based on Swarm Intelligent Ant Colony Optimization Technique

Ankush Parashar[1], Parveen Kakkar[2]
Research Scholar[1], Assistant Professor[2], Computer Science Department DAVIET, Jalandhar, India

Abstract: SYN flooding attacks still dominates the DDoS attacks. These attacks utilize the vulnerability in connection establishment phase of TCP. The attacker exhaust the limited resources of the victim server by continuously sending a large number of TCP SYN requests towards the server and does not respond to the SYN requests send by server which causes exhaustion of the server resources. During attack major part of the TCP buffer space is allocated to the attack requests and new connection requests are blocked. This paper proposed an SYN flooding DDoS attack Defense scheme based on Swarm Intelligence technique, which uses the Ant Colony Optimization algorithms to optimize the control parameters of the victim server so that it decreases the attack requests from the buffer space also a Data Protection technique integrated with this framework to provide overall security for the wired network by blocking the attacker which is flooding the victim server with SYN packets. Our simulation and analysis of proposed work in ns-2 environment shows that the proposed scheme is improving the results by decreasing the TCP connection loss and the share of attack requests from the buffer space.

Keywords: DDoS, Ant Colony System, Encryption, SYN Flooding attack, Swarm Intelligence,.

I. Introduction

Transmission control protocol based services are used in majority internet applications. DDoS attacks make the server unavailable for its legitimate users by making them so busy in handling the attacker as a result of which its resources get exhausts then server keep on denying the legitimate users. TCP SYN flooding attack uses the TCP architecture to launch the attack. In this the attack, the attacker floods the server with SYN requests and server allocate some resources like buffer space in its Transmission control block (TCB) to handle the connection details. Attackers sends number of SYN packets towards the server to occupy the server resources and does not reply to the server response. So there will be more half open connections in the TCB. As the server have limited resources so at some point of times the server resources get exhausted and now if any user sends request to make a connection with the server it will simply denies the request [1].

In some situations the attacker hides its identity by using the spoofed SYN flood attack. In this the attacker does not uses its own computer to launch an attack it uses the Bots or Botnet to launch SYN flooding attack on any server. Attacker infects these computers called bots and if a network of Bots is present then it is called botnet. Attacker can control these bots and used them to launch an attack. So in these types of attacks it is very difficult to find the attacker. It has been shown that more than 90% of the DoS attacks use TCP [2].The two main reasons to use to TCP are the vulnerabilities in the TCP. The First is, TCP does not have control over the clients which can send the SYN requests to any server. Second is that is allocate the resources to client before the final handshake.

The primary objective of the proposed work is to defend against the TCP SYN flooding attack on wired networks. As during the attack the buffer is full with the more number of half open connections and less number of regular connections. So we have taken this as optimization problem and solve it using the ant colony optimization algorithms. Which optimize the parameters of victim server so that there would be less number of attack connection inside the buffer and more number of regular connections and also there will less connection loss during attack. Also to provide over all security we have integrated a security scheme with ant colony optimization algorithm which securely send the data by hiding the data in data transfer phase of TCP three way handshake procedures. The rest of paper is organized as follows: section II shows the related work. Section III describes the TCP SYN flooding attacks. The proposed scheme discussed in section IV. Section V describes Simulation Results and Discussion and section VI concludes the paper.

II. Related Work

DDoS attacks shows about growing threats to businesses and Internet providers around the world. While many techniques have been proposed to detect these attacks, they are either not efficient or not effective enough. Even though lot of efforts has been made to provide defense from these attacks in the field of detection and prevention in network security but still they are serious problems on the internet yet. In terms of prevention, approaches like egress [3] or ingress filtering [4], disabling unused services [5], and honey pots [6]. Other approaches like backscatter analysis [2] and a router based technique [7] is also used to detect DoS attacks.

Authors of [8] proposed a technique to defend against SYN Flooding attack using particle swarm optimization. They have taken the problem as an optimization problem and solved it with the particle swarm optimization algorithm. Authors of [9] proposed a solution to mitigate the effect of DDoS attack using Swarm intelligent water drop algorithm. Intelligent water drop is used to get the path from which water drop(packet) can go with less soil(delay). GA's Crossover is used to get the node with maximum speed in swarm nodes. Comparison are done of number of connections between network with Swarm and without swarm nodes. Parameters over which comparison is done is PDR. Authors of [10] proposed the work to detect the SYN Flood attacks with WSAND algorithm using Net flow data at the live network border. They have worked against Netflow because with the IPv4 exhaustion dark net is difficult to get so net flow is used. A complete scenario of position of attacker, a victim and attacking address is designed. Total eight positions are designed. Then algorithm WSAND to detect attack is proposed. They have used SYN/SYN+ACK pair.

Authors of [11] presented an algorithm to detect the SYN Flooding attacks in Mobile Ad hoc Networks at early stage using game theory. Malicious nodes delay the communication before launching the SYN Flood attack. This technique is exploits to detect the malicious node in Mobile Ad hoc networks. This algorithm forms a game between the malicious node and multimedia server. The robustness of algorithm is check by using parameters related to the multimedia communication Authors of [12] proposed an algorithm for detection and defense against SYN Flooding attacks in SDN. SLICOTS is the name of the algorithm that is implemented at the Control plane of the SDN which effectively install the rules to OF Switch at the time of attack and secure the network. The authors of [13] proposed an algorithm based on the windows advanced firewall rules. They enhance the capabilities of firewall and proposed an algorithm to detect and mitigate the effect of SYN Flooding attacks. It is a three-way counter algorithm and uses the honey pots based scheme. The results show that 97.5% identification, detection and mitigation using proposed technique. In [14] author have proposed a scheme Largest Processing Time Rejection- Particle Swarm Optimization (LPTR-PSO) which defend from SYN flooding attack by scheduling the resources to SYN requests. Author proposed a scheduling algorithm which helps assigning resources to the requests in a particular order based on various parameters such as priority, processing time, etc this scheduling algorithm identifies the harmful requests and rule them. Author of [15] have presented Efficient Spoofed Mitigation Detection Scheme (ESMDS) which uses the TCP probing method along with the bloom filter trust model. The proposed scheme provides accurate and robust information for the detection and controlling of the spoofed packets, during the DDoS attacks. This paper detects and mitigates the SYN spoofed flooding attack.

III. TCP SYN Flooding attack

TCP is a connection oriented, reliable protocol used to send the data from one system to another. Application which uses the TCP based services need to make the connection first and then data will be transferred. So the TCP works in three way handshake procedure to make the connection. The three-way handshake protocol works as follows

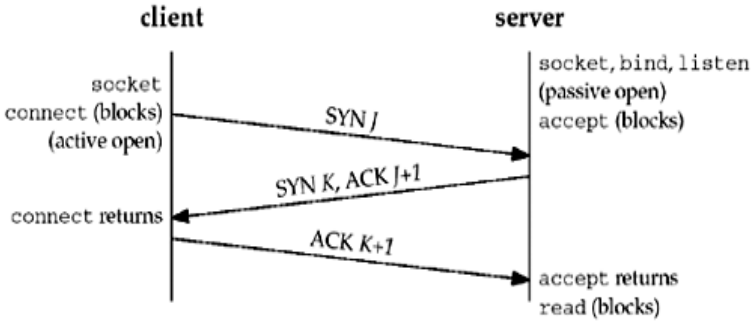

Figure 1 TCP three ways Handshake Procedure

- A client sends a SYN packet to a server to perform an active open request
- The server reserves connection resources (backlog queue) to track the TCP state on receiving a SYN packet and replies with a SYN/ACK packet in response.
- Finally, the client sends an ACK back to the server as an acknowledgement, and the connection is established when receiving this ACK on the server side.

During SYN flood attack, the attacker sends number of SYN requests to the server but does not send the final ACK to complete the connection also server allocates the resources to requests and many connections will be left half open. So in this way resources of server got exhausts and now server denies the requests from the legitimate users. In this way this attack is launched. There are three types of SYN flood attacks [16], which are going out in the nowadays Internet networks: Direct Attack, Spoofing Attack and Distributed Direct Attack.

1) **Direct SYN Flooding attack:** If attackers rapidly send SYN segments without spoofing their IP source address, this will cause direct attack. One way to perform this type of attack is by simply using many TCP connect () calls. However, the attacker's operation system must not respond to the SYN-ACK.
2) **SYN Flooding Spoofing attack:** On the other hand, in the SYN spoofing attack uses IP address spoofing, which might be considered more complex than the method used in a direct attack. During this type of attacks the attacker will sent SYN packets spoofed with the legitimate user source address to victim and then victim will respond with SYN-ACK to the legitimate user. IP address spoofing techniques can be categorized into different types according to what spoofed source addresses are used in the attacking packets.
3) **Distributed SYN Flooding DoS Attack:** A distributed SYN flooding attack is the most dangerous amongst mentioned types of SYN flooding attacks. During this type of SYN flooding attack the attacker takes advantage of numerous zombie machines/processes throughout the Internet. In the case, the zombies use direct attacks, but in order to increase the effectiveness even further, each zombie could use a spoofing attack and multiple spoofed IP addresses. Currently, distributed attacks are feasible because there are several "botnets" or "zombie armies" of thousands of compromised machines that are used by criminals for DoS attacks. Because zombie machines are constantly added or removed from the armies and can change their IP addresses or connectivity, it is quite challenging to block those types of SYN flood attacks.

IV. Proposed SYN Flooding Defense Method

The proposed work for defend against SYN flooding attack for wired networks consists of two phases, First phase is to design Proposed SYN flooding DDoS attack Defense scheme which defend from SYN flooding attack on wired network and second phase is to provide overall security to the network. To model this attack, we consider only one resource i.e. the memory space of the victim server and it has limited capacity is considered as a queuing system. Employing queuing theory, we give modelling of SYN flooding attack. In this model, all connection requests share a same backlog queue. When a request arrives at the system, then server must allocate a fixed buffer space to the connection so that it can transfer the data of size equal to that of the buffer.

Assume that there are two parameters of the victim server. First is, each half open connection is held for maximum time of c seconds and maximum d simultaneous half-open connections are allowed. So when the system is under attack the number of half open connection increase which led to consumption of resources of server and hence blocking all the legitimate requests. So the number of pending request will increase. Now for the larger value of c the number of half open connection will remain in the queue for longer time and if we decrease the value for c then time for half open connections will get decreased and the number of half open connection requests will decreases from the queue. Also by increasing the value for d we can make room for new connections which were denied. Therefore optimization of these two control parameters is necessary. So values of d and c are the important control parameters. In proposed work we optimize theses control parameters using Ant Colony Optimization techniques and evaluate the effect of optimization of parameters on the victim server. The optimization is done by some objective function. The system performance is measured continuously and an objective function is formulated and Optimization of parameters is done w.r.t. an objective function, in other words, System will be defended from attack by optimizing the parameters so that the number of attack requests inside our queue, the packet loss will be minimized and the number of regular request are maximized. These parameters are defined as follows:

ARBOP (Attack requests buffer Portion) is the number of attack requests inside the buffer, ie the half open connections which are closed after c seconds are regarded as attack connections.

RRBOP (Regular requests buffer Portion) is the number of regular requests inside the buffer, ie the half open connections which are closed before c seconds are treated as regular connections. A numbers of such packets are noted down for the victim system for both the Attacks request and regular requests.

Ploss (Packet loss) is the number of connection loss (SYN Packet Loss when the victim's resources are exhausted). It must be less for an ideal network.

The queuing theory is used for modelling the problem, in which, the connection requests are queued, waiting for the service. The complete model for proposed work is explained in the Figure 2. The two phases of proposed work used in TCP three way handshake procedures. The First phase works in connection establishment phase and the second phase which ensures the data security will work in data transfer phase of TCP three way handshake procedures. There are two types of packets in our approach: data packets and ant (or control) packets. Data packets are the data carried in the wired network. The routing algorithm routes these packets from the source to the destination, but has no interest in the contents of these packets. Forward and backward ants named ACO F and ACO B, respectively, are represented by control packets. These control packets updates the pheromone values and send them to proposed SYN flooding DDoS attack Defense scheme. A Data Protection Scheme (DPS) secure the data by encrypting the data using a dynamic key generated by the algorithm. This data protection scheme will be integrated with the proposed scheme.

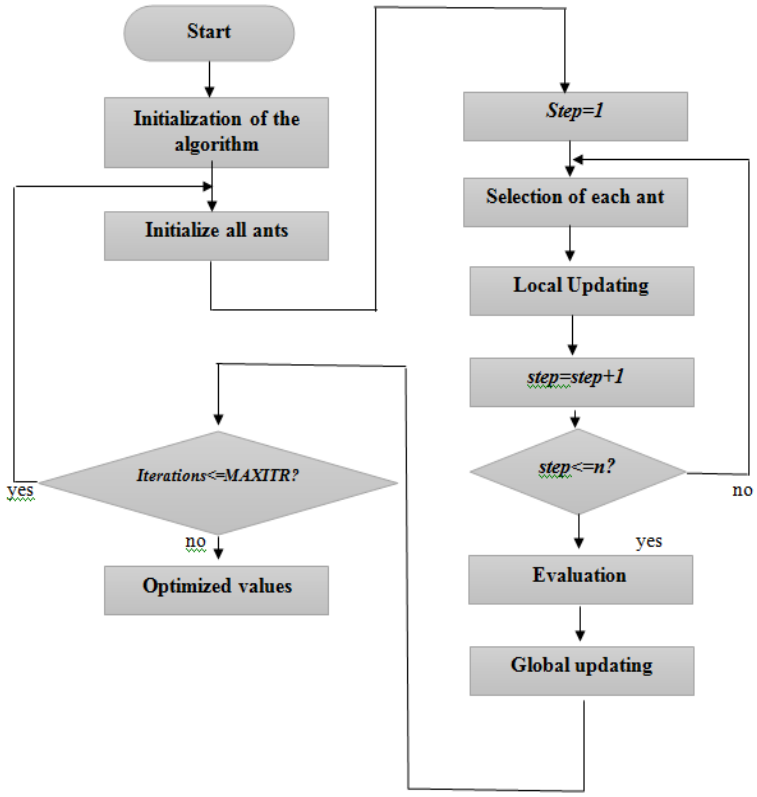

Figure 2 Flowchart for Proposed Work scheme

In the Figure 2, flowchart of proposed approach is given. The first step is to initialize the algorithm and all ants then iteration for local update of pheromone is done by each ant. Local pheromone updates diversify the search so that the later ants take their decision for choosing particular path. After all iterations all ants have completed their solution then an optimal solution is made based on the evaluation and then ants do global update. A new set of control parameters values are obtained which will be applied to the under attack system. This process will goes on and system is monitored for each iteration. New set of control parameters are assigned to system which results decreased number of attack connection, connection loss, and increase in regular connections.

In our scheme, the first phase is to find the optimal values of two control parameters through an ACO, based technique. On this basis, each ant tries to find a path in the network by providing minimum cost. Ants are initiated from source node *s*, move through neighbour nodes *di*, and reach a final destination node. As shown in (1), the choice of the next node *d* is made according to a probabilistic decision rule proposed in the ACO metaheuristic.

For each ant *k* at *i* has the probability for choosing the *ij* edge is

$$q^{k}_{ij} = \begin{cases} \frac{\tau_{ij}^{\alpha} \cdot \eta_{ij}^{\beta}}{\sum_{c_{il} \in N(s^p)} (\tau_{il}^{\alpha} \cdot \eta_{il}^{\beta})} & if\ c_{ij} \in M(w^p) \\ 0 & Otherwise \end{cases} \quad (1)$$

Where, $\alpha \geq 0$ is a parameter to control the influence of τ_{ij}. $\beta \geq 1$ is a parameter to control the influence of η_{ij} . τ_{ij} and η_{ij} represent the attractiveness and trail level for the other possible state transitions. M (w^p) is the set of feasible components; that is, edges (i , l) where l is a node not yet visited by the ant k.
During ant's exploration, forward ant (ACO_F) will collect all the information of the paths passed by, while backward ant (ACO_B) recoiling back from a destination node to a source node s. During its moving back, ACO_B will update the pheromone values of all the nodes along the path according to the information collected by the corresponding ACO_F. Each ant has the memory which contains the already visited nodes, by exploiting this ant's memory; an ant k can build feasible solutions. On this, no node can be visited more than once. At each node d, a forward ant selects the next hop node using the same probabilistic rule proposed in the ACO metaheuristic [16]. The visibility function or heuristic function is given by

$$\eta_{ij} = \frac{RRBOP}{(Ploss \cdot ARBOP)} \quad (2)$$

It is the objective function its value should be high as to optimize the parameters the RRBOP should increase and Ploss and ARBOP should decrease. If this happened only then our heuristic function will give maximum value. We have to maximize this function i.e. maximize RRBOP and Minimize Ploss and ARBOP.
Once a forward ant reaches the destination node, it is transformed in a backward ant with the aim of updating the pheromone trail of the path it used to reach the destination and that is stored in its memory. This update will be computed by the destination node through this formulaThe local pheromone update will be done by ant at i is for all iteration by using the following equation.

$$\tau_{ij} = (1 - \varphi) \cdot \tau_{ij} + \sum_{k} \Delta\tau^{k}_{ij} \quad (3)$$

Where, τ_{ij} is the amount of pheromone deposited for a state transition i to j. $\varphi \in (0, 1]$ is the pheromone decay coefficient, $\Delta\tau^{k}_{ii}$ is the amount of pheromone deposited by k^{th} ant, It diversifies the search performed by the ants so that others ant doesn't choose same edge and it encourages subsequent ants to choose other edges.

Our proposed work has one additional feature which secures the data of clients by hiding the data and also blocks the SYN flood attacker. This feature in the proposed work will ensure the overall security of our wired network. In this approach every node will use a public key encryption method to generate the keys to encrypt the packets before sending to start data transmission. Every node needs to send SYN packets initially. New algorithm will set a timer of 'x' seconds. The value of 'x' will be encrypted using that key. At the server the value will be decrypted. Any node cannot send packets for more than 'x' seconds. Server will decrypt the packet and see the value. The server will accept SYN packets for 'x' amount of time. If any value is more than 'x', then node will be blocked for further communication. So using this method the data is send in encrypted form, from source to destination in other words the data is hidden from the outside world and not everyone can read the content of that data. This is done at data transfer phase of TCP three way handshake procedures. Also this scheme will block the attacking server so it overall securing the network from attack.

As the TCP is a connection oriented protocol. It makes a connection before transferring the actual data. During the Connection establishment phase of TCP, Ant colony based algorithm is used for optimization of parameters using proposed scheme it gives the optimal values of control parameters which reduces the SYN flooding DDoS attack. To provide overall security for the network, data should be secured so additional feature is added to the proposed scheme which hides the data and blocks the attacker in network.

V. Result and Discussion

In this section the proposed work is compared with the Existing method (PSO_SYN), In the first round of simulation the system is configured without any attack (i.e. Linux TCP) and its performance is measured in terms of parameters like ARBOP, RRBOP, Ploss, Queue length, Buffer size. Then in next round simulation, performance is measured with the system configured under SYN Flooding attack. Then system is configured with the Existing protocol and performance is measured. The same simulation is done with the proposed scheme. Then comparison results for each parameter are shown in this section.

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 9 • Issue 2 pp. 19-27 March 2018 - Sept 2018 www.csjournals.com

6.1 ARBOP

There are two types of SYN requests present in the buffer, regular requests and attack request. ARBOP is the number of attack requests present in the buffer i.e. connections which are closed after the h seconds. For a network free from SYN flooding attack, ARBOP value must approach to zero. Buffer space is monitored each second during the simulation and ARBOP is measured for normal scheme, attack scheme, existing scheme and for proposed scheme. A comparison graph is plotted as shown in the figure 3.

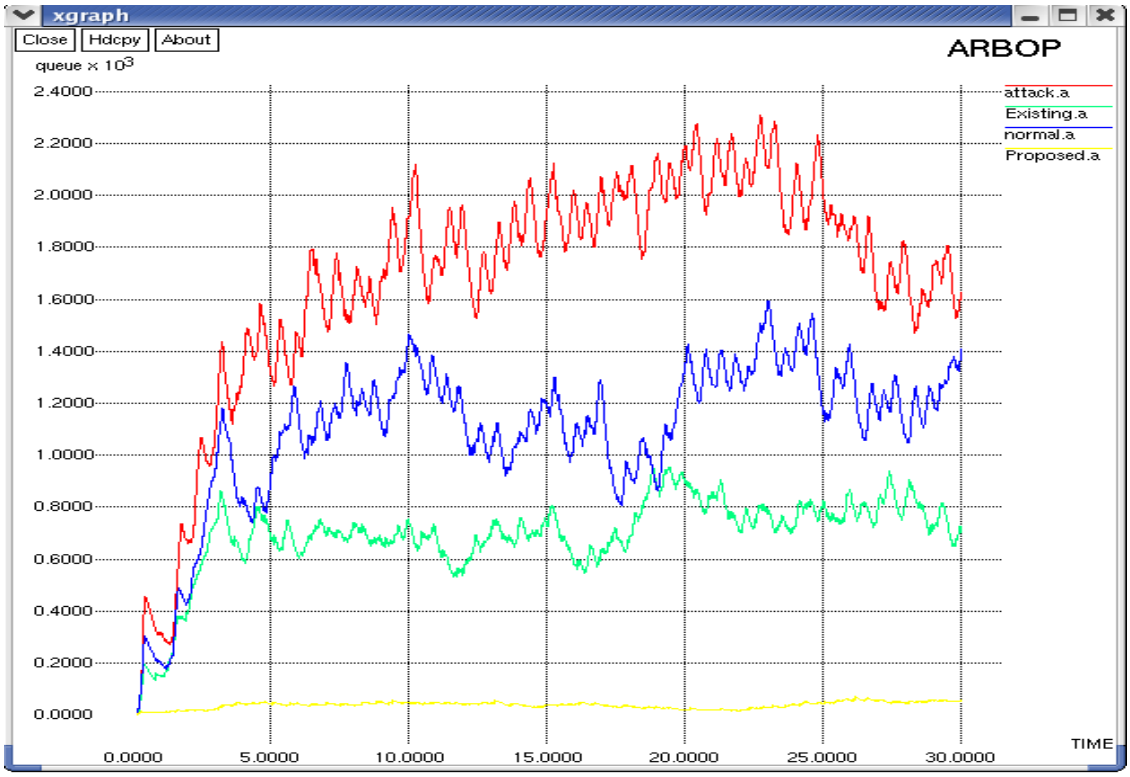

Figure 3 Attack Request Buffer Occupancy for Proposed and Existing work

In figure 3 if we see that during normal operation some attacks requests are there as it is supposed to show nil. It is because of the fact that we are taking the request which closes (completes the third leg of handshake) after *c* seconds as attack requests so during normal operation there may be some requests which are closed after *c* seconds. That is why showing deflection in graph for attack requests is. During simulation for attack, its value becomes higher than normal. Our proposed scheme is decreasing the share of attack connections from buffer space, comparing to Existing scheme. it is clear that the proposed scheme certainly improving over the existing scheme.

6.2 RRBOP

RRBOP is the number of regular requests present in the buffer i.e. connections which are closed before *c* seconds. This is measured by monitoring the buffer space. As according to our objective function, the control parameters dynamically tunes by proposed scheme so that our RRBOP increases. The numbers of regular requests present in the buffer during attack RRBOP under the proposed scheme are more than for existing scheme.

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Volume 9 • Issue 2 pp. 19-27 March 2018 - Sept 2018 www.csjournals.com

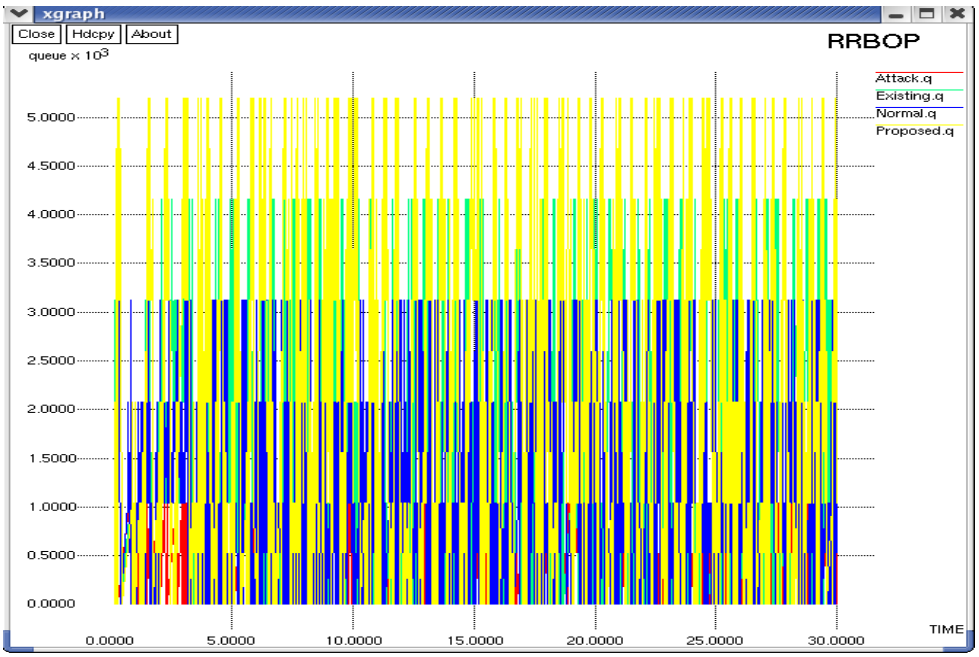

Figure 4 Regular Request Buffer Occupancy for Existing and Proposed work

6.3 Ploss

It is the number of connection lost or packet loss, connection loss is the number of dropped requests (SYN requests when system resources are exhausted), the requests come after when *d* concurrent connections are there. For an ideal connection its value must be less. Ploss values are measured each second for existing scheme and proposed scheme and Comparison graphs are plotted. Our proposed scheme shows great performance as compared to existing scheme. It lowers the Ploss.

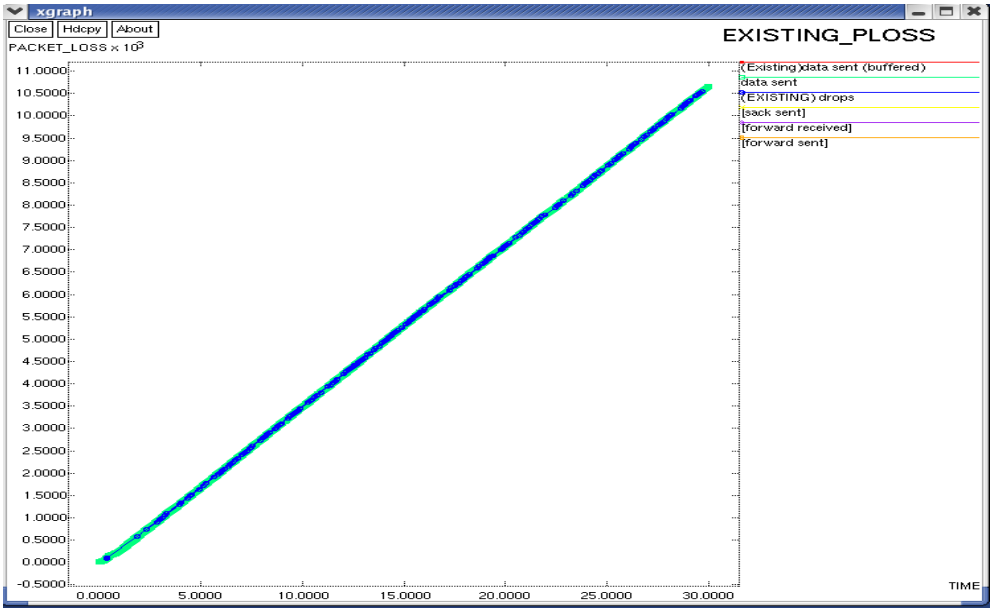

Figure 5 Ploss for Existing Work

Figure 5 shows the packet loss for existing work. Its value rise up to 11K packets while the proposed work improves the performance by applying the proposed approach which reduces the number of connection loss in tcp handshake procedure. The proposed scheme decreases the value of packet loss to 5K SYN packets requests as shown in the figure 6.

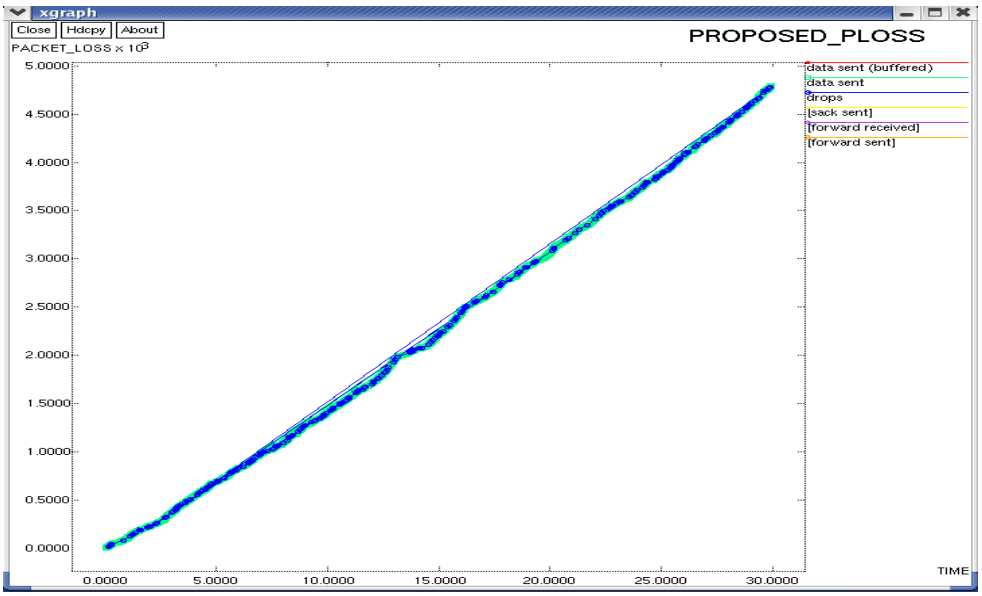

Figure 6 Ploss for Proposed Scheme

By applying the proposed scheme the value of *d* will dynamically increases which cause the more number of half open connection held at a time so whenever a new request comes it will be in queue for regular requests and packet is not discarded and hence less packet loss.

VI. Conclusion and Future scope

This paper proposed an approach to defense against the TCP SYN flooding attacks on wired networks. A swarm intelligence based ant colony optimization is used in proposed work which tries to reduce the share of attack half open requests from the buffer of TCP. It also reduces the connection loss during the TCP SYN flooding attack and to overall secure the network an additional feature is implemented which secures the data of user by hiding the data and blocks the attacker from network. Queuing theory is used to demonstrate the attack situations. The ants based scheme works at connection establishment phase while the Data Protection scheme works in data transfer phase of TCP. The defense problem is taken as optimization problem which optimize the control parameters with respect to some objective function. Proposed scheme dynamically changes the values of control parameters and place them on best defense positions. Under attack system is continuously monitored and performance parameters are measured. This research shows that our proposed scheme remarkably improves the performance of under attack system than the existing scheme. As for future work similar meta-heuristic techniques like genetic algorithms to design the defense mechanism can be employed also the buffer allocation strategies can be modified to improve the defense schemes.

References

[1] Geetha K, Sreenath N. Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol. Springer: Arabian Journal for Science and Engineering. 2016; 41(3):1161 72.

[2] Moore D, Shannon C, Brown D, Voelker G, Savage S. Inferring internet denial of service activity. Trans Comput Syst 2006:115–39.

[3] Ehlert S, Geneiatakis D, Magedanz T. Survey of network security systems to counter SIP-based denial-of-service attacks. Comput Secur 2010; 29(2):225–43

[4] Yu CF, Gligor VD. A formal specification and verification method for the prevention of denial of service. In: IEEE symposium on security and privacy proceedings; 1988. p. 187–02.

[5] Warrender BPC, Forrest S. Detecting intrusions using system calls: altemative data models. In: IEEE symposium on security and privacy; 1999. p. 133– 45.

[6] Hussain A, Heidemann J, Papadopoulos C. A framework for classifying denial of service attacks. USC Information Sciences Institute; 2003. p. 99–110.

[7] Vulimiri A, Agha GA, Godfrey PhB, Lakshminarayanan K. How well can congestion pricing neutralize denial of service attacks? SIGMETRICS Perform Eval Rev 2012:137–50.

[8] S. Jamali and V. Shaker, "Defense against SYN flooding attacks: A particle swarm optimization approach," Computers & Electrical Engineering, vol. 40, no. 6, pp. 2013–2025, 2014.

[9] Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.

[10] Miao, L.; Ding, W.; Gong, J. A real-time method for detecting internet-wide SYN flooding attacks. In Proceedings of the IEEE International Workshop Local and Metropolitan Area Networks (LANMAN), Beijing, China, 22–24 April 2015; pp. 1–6.

[11] Geetha K, Sreenath N. Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol. Springer: Arabian Journal for Science and Engineering. 2016; 41(3):1161-72

[12] R. Mohammadi, R. Javidan and M. Conti, "SLICOTS: An SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks," in *IEEE Cdansaccions on Necwodk and Sedvice Managemenc*, vol. 14, no. 2, pp. 487-497, June 2017.

[13] Hussain, Khalid, et al. "An Adaptive SYN Flooding Attack Mitigation in DDOS Environment." *IJCSNS* 16.7 (2016): 27

[14] Ahmed, Zonayed, Maliha Mahbub, and Sultana Jahan Soheli. "Defense against SYN Flood Attack using LPTR-PSO: A Three Phased Scheduling Approach." *INCEDNACIONAL JOUDNAL OF ADVANCED COMPUCED SCIENCE AND APPLICACIONS* 8.9 (2017): 433-441

[15] Kavisankar, L., et al. "Efficient SYN spoofing Detection and Mitigation Scheme for DDoS attack." *Decenc Cdends and Challenges in Compucacional Models (ICDCCCM), 2017 Second Incednacional Confedence on*. IEEE, 2017

[16] Bogdanoski, M., Shuminoski, T. and Risteski, A., 2013. "Analysis of the SYN flood DoS attack". *Incednacional Joudnal of Compuced Necwodk and Infodmacion Secudicy*, 5(8), p.1.