Ant Colony Traceback for Low Rate DOS Attack

M. Hamedi-Hamzehkolaie
Kish international campus
Tehran University
Iran

M. J. Shamani
Kish international campus
Tehran University
Iran

M. B. Ghaznavi-Ghoushchi
School of Engineering
Shahed University
Tehran, Iran

ABSTRACT
Denial of service is one of the most common threats on the public open networks like Internet which taken up by spoofing in the IP address source and leads to exploit the system resources. This results in a decline in the system performance and normal response. In this paper, the traceback to intruder approach by ant colony algorithm will be applied. And the variance of flow will be used to traceback the Denial Of Service or DOS attack source based on ant colony and metaheuristic algorithms. The simulation results show that the proposed approach can trace the attacks even if the attack traffic intensity is relatively low and by initializing the algorithm parameters correctly. Our simulations show that the probability of errors will reach to its lowest rate or even to zero and this is considered as an effective step in tracing attacks by means of metaheuristic algorithms.

General Terms
Network security

Keywords
Denial of Service, Ant Colony, Traceback, Metaheuristic algorithms, Network Traffic.

1. INTRODUCTION
According to the annual security infrastructure report [1] in 2010 and the report of cryptic assembly [2] in 2012 the frequency of denial of service attacks has been doubled per year of the decade and related to that damage and threats are increasing every day. Low traffic attacks are almost 80 percent of DOS attacks [1], which mitigating are relatively more difficult [3].

On the other hand, counter techniques are categorized into defense and detection [3]. In order to defend against DOS attacks traffic control mechanism such as packet filtering based on route [4], ingress filtering [5] and rate limiting are proposed. However, rate limiting [6] is not suitable for mitigating attacks having low-data-rate on a link, since these attacks will not trigger rate limiting operation [3].

All the above mentioned approaches are passive since they cannot fully resolve the problem. However, proactive approaches [7] will try to find the attack sources under the control of Internet Service Provider (ISP) or the network administrator supervision. Then it will block the traffic from the source and become able to stabilize the network service and will finally end in arresting the intruders.

Current Internet protocol (IP) traceback approaches like: Probabilistic packet marking [8], Hash [9] and Hop by Hop [10], use the information of the routers along the DOS path. However most of previous approaches, in order to, encrypt the routers information on IP headers or storage of the quantity and amount of package volumes on the routers or IP address traceback aims need to provide infrastructures in the network. In addition to that, to succeed in tracing the IP address of the denial service we need the support of all routers.

Among other approaches of finding the IP address of the DOS attack source, which have been discussed, one is the traceback via considering the network current traffic flow information or applying ant algorithm [11]. For example, in [15] a traceback method that is based on entropy variance has been presented.

Nevertheless, few heuristic algorithms are studied in IP traceback. The heuristic algorithms are naturally very strong at finding the optimal result. The nature of these kinds of algorithms is searching food to survive, similar to the nature of IP traceback [11-13]. Some researchers simulated and designed network topology using their favorite approach [14]. Similarly, most approaches considered by researchers are applied for those networks with intensive traffic attack. Also in [12] using the ant colony algorithm has been proposed where the attacker is placed in the middle hop.

Furthermore, analyzing attacks with low rate traffic has been done in "ITACS" [16]. Nonetheless, this approach which has been developed for fixing others drawbacks still shows drawbacks in this kind of traceback. Low rate traffic attack has also been analyzed by the authors of this paper in [17] by applying level of flows.

The proposed method in this paper has three main differences with other methods in this field. The first one is, it can be applicable for low rate dos attack, apart from being applicable for intensive traffic attacks as usual. The second one is, applying flow variance in our traceback method which to the best of our knowledge has never been used so far. The third one is that, the maximum number of converged ants in summation of all algorithm iterations has been considered to find the target node.

The outline of the paper is in the following manner: In section 2, we describe the proposed model. In section 3, the algorithm flowchart has been presented. In section 4, simulation and result have been shown, finally in the last section, we conclude the paper.

2. PROPOSAL MODEL
In this model we tried to improve ant colony trace back algorithm [11] in order to trace not only high traffic attacks which are easy to traceback but also low traffic attacks which are important because of their current growth and apart from it are difficult in case of quantity and complexity.

2.1 Schematic system of ant colony algorithm
When a large number of ants follow a sequence, it usually attracts more ants. In the proposed IP finding plan, we have used the average number of existing octet belong to denial of service as Pheromone effect. Therefore, the router with more traffic and more flow of denial of service will be selected by