Attack Prevention and Attack Detection Strategies by Comparing different DDos Models

Siva Balaji Yadav C.
Research Scholar
SVU College of Engineering
SV University, Tirupati-India

R. Seshadri, PhD
Director
SVU Computer Center
SV University, Tirupati-India

ABSTRACT
DDoS attacks are launched with the intention of depleting the network and server resources. The proposed work identifies that the malice behavior of the nodes requesting service and the malice nature of the traffic are the two major issues to be addressed. Accordingly, the defense framework employs attack avoidance methods, attack prevention model and attack detection strategies to be deployed in each autonomous system (AS). A way of avoiding attacks is to ensure that attacks may not exploit the vulnerabilities. This is achieved in this work through enhanced anti-spoofing techniques that resolve insider attacks, and a differentiated routing based on traffic classification.

Keywords
DDoS, Attack detection, Autonomous system, anti-spoofing.

1. INTRODUCTION
Many trust models have been proposed in the literature for different application domains. There is a strong correlation between trust models and optimism [1,2]. Trust model should depict the interrelationship between the entities involved in establishing trust and the techniques used to evaluate trust using appropriate metrics. This chapter describes a secret agent based behavior trust model to make the network less liable to general security attacks and denial of service attacks in particular. The proposed model characterizes not only the behavior of traffic generated but also the behavioral changes in generating the traffic and responding to control activities in the network [3, 4]. It is found to be appropriate that the behavior of the source nodes that generate the traffic may be taken into account to predict the traffic characteristics that is being generated by them as belief is a critical component in trust evaluation. The Internet, a network of networks, can be viewed as a hierarchical structure with the hosts of various subnets at the outer layer connected with each other through the network core via edge router elements. The hosts talk to each other via the routers to which the hosts' subnet is connected and that in turn talk with the peers at various levels of network backbones [5-8]. During data transmission between two hosts A and B, the minimum set of elements that participate include the two edge routers connected to the two subnets to which A and B belong to, other than the two hosts A and B [9]. The proposed framework that defines a solution to the DDoS attack for identifying reliable elements to participate in data transmission, make out two sets of elements as drafted above as the elements to be focussed for enforcing network sustainability [10]. They are the subnet nodes N1, N2, N3 and N4, which originate data transmission by way of requests and first level routing elements R [11]. Since these border routers got fed by the subnet nodes or hosts, it is more logical to consider the verification of data sources for reliability based on their behavior.

2. METHODOLOGY
Trust is multi faceted entity, and choosing the most appropriate parameters for evaluating trust are context based. The trust model proposed in the thesis work is behavior based model where the trustworthiness is evaluated based on the parameters of neighborhood sensing behavior and traffic generation behavior. All legitimate client nodes are assumed to be credible in conforming to the router query response protocol during neighborhood sensing. Neighborhood sensing is incorporated using a simple query-response protocol that employs returning IP as neighbor feedback. This reduces the message overhead involved in collecting recommendations from neighbors.

Mutual trust is one of the laws of nature that runs the universe. In harmony with natural laws one component of trust metric is defined to be the trust value evaluated by the neighbors. It is assumed by the reciprocity nature of trust that a trustworthy neighbor returns no false reply about its trustworthy neighbor. In general, any node more specifically an attacker node may not be trustworthy in returning the real trust of its neighbors. So, in order to nullify the effect of false reply, a deterministic binary event probability model is proposed as detailed below.

The set of the nodes in the subnet are defined using cross partition as follows:

Let S1= {TN, NTN} be the set of trusted nodes and non-trusted nodes in a subnet routed via a router as updated by the comparator. Let S2 = {1,0} be the set, representing the values returned corresponding to the probe request sent and value is 1 when sending true IP and 0 for sending false IP or no reply. The cross partition set between S1 and S2, represented as S1× S2 is defined below.

S1× S2= {(TN,1),(TN,0),(NTN,1),(NTN,0)} defines the set of TN nodes that return true, the set of TN nodes that return false, the set of NTN nodes that return true and the set of NTN nodes that return false respectively. For node X, the cross partition set is defined as X:S1× S2 = {X:r1,X:r2,X:r3,X:r4} where r1,r2,r3 and r4 are subsets contained in S1× S2 . The cardinality of the cross partition is defined as the number of nodes that satisfy the condition in the cross partitioned set. Trust for the node X is evaluated using the response sent for the neighbors and response received from its neighbors and is detailed as follows. It is assumed that the behavior of all the nodes are equi-probable in sending true value to its neighbors and the node's response is modeled as a binary event.
Trust Returned by Neighbors

The trust evaluated for node X based on its neighbors' reply is described here. Let x1 be the number of trusted neighbors of X who return 1 for X and similarly x2 defines the number of trusted neighbors of X who return 0 for X and x3 and x4

represent the number of non-trusted neighbors of X who return 1 and 0 respectively for X through PRBrep. So the cardinality of the set X:S1× S2 is x1+ x2+x3+ x,where x1 is the cardinality of the first element in the cross partition set, i.e. subset X:r1, x2 is the cardinality of the subset X:r2, x3 is the cardinality of the subset X:r3 and x4 is the cardinality of the subset X:r4. The first component of trust for the node X is evaluated using Equation (1), where the factors α1 and β1 represent the degree of trustable behavior returned by set of trusted and non-trusted neighbors of X.

Trust received X α1 (X1-X2) + β1 (X3-X4)

The probability pi1 for the node i to return 1 for X is predefined based on the neighborhood topology and ni1 is the number of times the client I returns 1 for X during an observed interval of time t. The probability with the frequency of true/false response of α 1 denotes the average true value returned by the trusted neighbors and the difference between x1 and x2 defines the lower limit on the number of trusted nodes who return faithfully. Similarly β1 defines the average true value returned by the non-trusted neighbors and the difference between y1 and y2 defines the lower limit on the number of nontrusted nodes who return faithfully.

3. RESULT ANALYSIS

Simulation experiments were conducted to evaluate trustworthiness of nodes in a subnet based on the proposed behavior model. Evaluating the trustworthiness of nodes and finding the effectiveness in preventing the attack traffic is performed in two phases namely trust deduction using matching behavior for neighborhood sensing and trust assertion based on traffic generation behavior. Neighborhood sensing accounts for the two components namely trust sent and trust received while credibility factor is derived from traffic generation behavior. Probabilistic function is used in trust evaluation for addressing scalability of the network. The credentials for the users during trust evaluation were fixed based on the average bit-traffic generated with respect to the aggregated flow at the border router and so size of the packets used were not realistic. To have a stable aggregated flow for evaluation, the traffic generated by the users were assumed to be bursty in nature.

Analysis of the trust protocol for four different cases of behavior in a subnet was carried out.

(i) Malicious nodes, behaving illegitimate in neighborhood sensing and generating high rate traffic

(ii) Malicious nodes, behaving illegitimate in neighborhood sensing and generating low rate traffic

(iii) Malicious nodes, behaving legitimate normal in neighborhood sensing and generating high rate traffic

(iv) Malicious nodes, behaving legitimate normal in neighborhood sensing and generating low rate traffic

The study infers the following findings on the trustworthiness with respect to the two parameters considered. For the first two cases since the malicious nodes behave as malicious in responding for router queries, these nodes get listed as NTN based on the mismatching neighborhood information provided with reference to that collected by the agent and subsequently get deducted and the generated traffic rate is able to confirm the illegitimacy with varying time of detection.

During cases 1 and 2, the trust value for legitimate nodes and illegitimate nodes are observed as follows. For illegitimate nodes the low trust value evaluated is due to the reduced feedback received from legitimate neighbors and reduced trust sent for the trusted neighbors falsely as it is mismatched with agent information. For the legitimate nodes, trust received is lesser due to the illegitimate neighbors but trust sent is higher so that the overall trust is high. During the cases 3 and 4 since the illegitimate behavior is less and trusted nodes gain high trust while illegitimate nodes also earn more trust and this introduces false alarms. The testing topology is represented by the following adjacency matrix for nodes 1-8 in the topology.

3.1 Scenario 1: A single attacker in the subnet

Each node is generating data at varying rates between 104 to 106 packets with 500 to 1000 msec interval between packets of length around 100 bits and one node is considered to produce attack traffic at a higher rate of 104 packets of 100 bits with 1 msec interval between packets. Trust variations are recorded for a period of observation of 60 sec with average flow rate at router monitored at an interval of 10 sec. Node 5 is simulated to behave illegitimate for longer time than legitimate behavior.

Average rate of aggregated flow at router: 190 Mbits/sec.

Average trust at router: 5.9

Node	r 1	Trust-sent	Trust-received	Trust	Average trust
Legitimate node 1 Data rate 10 Mbits/sec	0.5	7.6	7.0	7.6	6.5
	0.55	7.6	7.0	7.7	
	0.5	7.6	7.0	7.6	
	0.55	7.6	7.0	7.8	
	0.6	7.6	7.0	7.9	
	0.65	7.6	7.0	8.1	
Attack node 5 Data rate 500 Mbits/sec	0.5	1	3	3	3.7
	0.45	1	3	2.6	
	0.4	1	3	2.3	
	0.35	1	3	2.0	
	0.3	1	3	1.9	
	0.25	1	3	1.7	

3.2 Scenario 2: Two attackers in the subnet

Scenario 1 is replicated with one more attacker added to the subnet.

Recorded trust values for a sample set of nodes in one of the periods of observation are provided in Table2

Average rate of aggregated flow at router: 259 Mbits/sec.

Average trust at router: 5.1

Node	r 1	Trust-sent	Trust-received	Trust	Average trust
Legitimate node 3 Data rate 100	0.58	5.3	5.4	5.8	5.4
	5.3	5.3	5.4	5.6	
	0.65	5.3	5.4	5.8	
	0.68	5.3	5.4	5.8	
	0.73	5.3	5.4	5.9	

Mbits/sec	0.72	5.3	5.4	6.0	
Legitimate node 5 Data rate 500 Mbits/sec	0.5	0	2.3	3.8	2.5
	0.45	0	2.3	2.7	
	0.4	0	2.3	2.2	
	0.45	0	2.3	2.7	
	0.4	0	2.3	2.2	
	0.35	0	2.3	1.5	
Legitimate node 6 Data rate 1000 Mbits/sec	0.5	0.4	4.2	5.1	4.3
	0.45	0.4	4.2	4.2	
	0.4	0.4	4.2	3.4	
	0.45	0.4	4.2	4.2	
	0.3	0.4	4.2	2.2	
	0.25	0.4	4.2	1.7	

The trust evaluated for the other nodes are 6.1, 5.6, 6.2, 5.4 and 6.4. Here nodes 2 and 7 have lower trust values among the trusted nodes due to smaller neighborhood size and node 7 has lesser value than node 2 as it has both attack nodes as neighbors. Since the attackers are simulated to behave legitimate also for a smaller period of time, the node 7 gets classified as legitimate else it will raise false alarm. It is observed through various runs of simulation that the attack node has been classified correctly as NTN before identified for getting dropped and the false alarm for the legitimate node getting classified as NTN is very less.

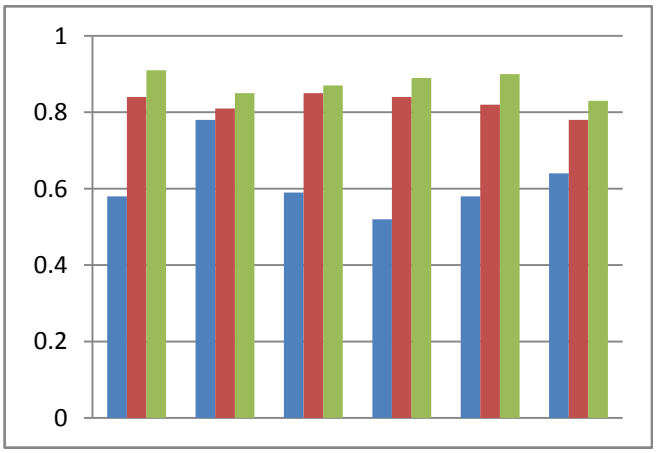

Fig 1: Trust values computed based on the behavioral profile

X-axis no of random nodes; Y-Axis no. of iterations

Switching between TN and NTN sets is observed to get stabilized once the attack has happened. This can be evaluated from the trust values computed based on the behavioral profile of the users, and the evaluation converges a little faster when the traffic profile is also considered as depicted in Figure 1. The marginal difference may get improved when tested with large network with many attack sources. When an illegitimate node generates low traffic, it takes a longer time to get identified. The overhead involved is, the deployment of the solution at all the border routers and sending periodic probe signals to monitor behavioral pattern but collaboration between border routers is very minimal.

4. CONCLUSION

The proposed behavior trust model is not intended to replace any of the research models available, instead it is intended to complement the existing models by demanding accountability for actions resulting in reduced trustworthiness for bad actions and labeling more weightage for good actions with less overhead. This boosts the nodes that participate in normal data transmission and penalizes the attack nodes whose participation is less as they are busy in attack packets generation. Most of the trust models use trust values that uses some method of probabilistic evaluation and deciding the base value is crucial for the effectiveness of the computed trust value. This may be subjective or context based information and the proposed method uses a topology based probability measure during trust computations. Opinion or suggestion also plays a role in the trust metric design and a formal mathematical model to perform trust transitivity is justifiable and hence the behavior based model uses neighbors' information along with secret agent information similar to psychometric analysis, to refine the trust parameters. The proposed model also supports scalability as it is localized to a subnet and hence scalable in the internet. From the simulations conducted, it is observed that the false negative is negligible and false positive is NIL as the system takes a sensible period of time to confirm the node in the non-trusted list as an attacker. The computational and storage overheads involved are negligible as the behavior is not stored for the past profiling periods, and the trust evaluation and updating are dynamic and dependent on the current values. The scheme is adapted to computational environments of any size as the solutions is deployed at the subnet level and is thus scalable. It is observed that when all the nodes in the subnet have comparable trusted neighborhood size, the trust variation between legitimate and illegitimate nodes becomes high leading to fewer false alarms.

5. REFERENCES

[1] Gil, T. M., and Poletter, M. (2001). Multops : a data-structure for bandwidth attack detection. Proceedings of US ENIX Security Symposium . USENIX Press, Berkeley, CA.

[2] Mahajan, R., Bellovin, S. M., Floyd, S., Ioannidi s, J., Paxson, V., and Shenker, S. (2002). Controlling high bandwidth aggregates in the network. ACM SIGCOMM Computer Communications Review , 32(3), 62-73.

[3] Li, J., Mirkovic, J., Wang, M., Reiher, P ., and Zhang, L. (2002). Save: source address validity enforcement protocol. Proceedings of IEEE Infocom , 3, 1557-1566. IEEE Press, New York.

[4] Gu, Q., Liu, P., and Chu, C. (2004). Tactical bandwidth exhaustion in ad hoc networks. Proceedings of the 5th Annual I EEE Information Assurance Workshop , 257-264. IEEE Press, New York.

[5] Zhang, R., and Chen, K. (2005). Improvements on the WTLS protocol to avoid denial of service attacks. Computers & Security , Vol. 24(1), pp. 76-82.

[6] Gu, Q., Liu, P., Zhu, S., and Chu, C. H. (2005) . Defending against packet injection attacks in unreliable ad hoc networks. Proceedings of IEEE Globecom . IEEE Press, New York.

[7] Aljifri, H., Smets, M., and Pons A. (2003). IP Traceback using header compression. Computers & Security , Vol. 22(2), pp. 136-151.

[8] V. Yegneswaran, P. Barford, and J. Ullrich. (2003) Internet intrusions: Global characteristics and prevalence. In In Proceedings of the 2003 ACM SIGMETRICS International conference on Measurement and Modeling of Computer Systems, pages 138-147.

[9] Y. L. Zheng and J. Leiwo. (1997)A Method to Implement a Denial of Service Protection Base. In Information Security and Privacy , volume 1270 of LNCS, pages 90-101.

[10] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic. (2000.) Distributed Denial of Service Attacks. InIEEE International Conference on Systems, Man, and Cybernetics , pages 2275-2280, Nashville, TN, USA.

[11] S. Savage, D. Wetherall, A. Karlin, and T. Anderson. (2000) Practical Network Support for IP Traceback. In Proceedings of ACM SIGCOMM.