Journal of Computer Science 9 (11): 1618-1625, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.1618.1625 Published Online 9 (11) 2013 (http://www.thescipub.com/jcs.toc)

DETERIORATING DISTRIBUTED DENIAL OF SERVICE ATTACK BY RECOVERING ZOMBIES USING PENALTY SCHEME

J. Udhayan and M. Rajesh Babu

Computer Science and Engineering, PPG Institute of Technology, Coimbatore, India

Received 2013-04-05, Revised 2013-10-05; Accepted 2013-10-09

ABSTRACT

Resource of victim impounded by DDoS attack leads the victim to series monetary loss apart from various other ill-effects. Already lot of solutions came up in technological aspects almost neglecting the economical aspects. Hence there is not yet a proper method to make the zombies accountable to the economical loss materialized as the effects of highly zombie oriented DDoS attacks. Therefore the need of the hour is to develop a prudential monetary based DDoS solution that serves as the economical defense as well as strives to bring heighted awareness among the zombies. Consequently in this study we discuss the techno-economical scheme termed as Penalty Scheme. This scheme is an idea of enforcing necessary means to evaluate the accountability of zombies which therefore serves as the economical defense towards the notorious DDoS attacks. This method notifies and makes the zombies aware of the loss incurred through their careless participation in DDoS attacks. The proposed scheme is analyzed using real time datasets, the results show the considerable improvement in the DDoS attack handling through integrating the Penalty Scheme with the cooperative filtering approach.

Keywords: DDoS, Zombie, Botnet, Cooperative Filtering, Decoy Network

1. INTRODUCTION

The DDoS attack is performed to deplete the resource of one or more victims and make it unavailable to the victim's legitimate client. Therefore it involves dumping packets from many zombies (compromised computers) towards the victim server (Gupta *et al*., 2011). Backbone of this kind of attack is the network of zombies called as decoy network or botnet. Even though zombie is termed as a secondary victim it is not the target of the DDoS attack but they act as the accomplice. In this study the zombie is coined as accomplice because at law, an accomplice is a person who participates in the commission of a crime, even though they take no part in the actual crime, such is also a punishable offence. The zombies though they not initiate the attack but they participate in the DDoS attack, therefore they are accomplice. Mostly the computers are compromised due to the lack of knowledge in security issues and lack of adequate security measures. The ignorance of zombies not only leaves room for DDoS attack but their own vital, private and sensible data are under risk of being exploited by the attacker at any time.

2. MATERIALS AND METHODS

This study reflect on the fact that considering the economical aspect of DDoS is esential to mutilate the attack. Therefore the limitations in existing techniques as well as the need to incorporate the fincial aspects are discussed as follows.

2.1. Technical Aspects

Most of the cases the DDoS attacks performed through exploiting the lack of authentication in the IP protocol and flaws in the protocols like TCP, UDP, ICMP, HTTP (Oikonomou *et al*., 2006). However the IP layer indeed transmits the information in the form of

Corresponding Author: J. Udhayan, Computer Science and Engineering, PPG Institute of Technology, Coimbatore, India,

packets, which can be counted and examined by the network entities and the victim itself (Akella *et al*., 2004). Therefore the steps in existing defense include detection and reaction mechanisms. These method works through counting and examining the packets. There are various methods proposed to detect the DDoS attack, however all this methods can either be classified as signature based or behavior based detection (Wang *et al*., 2007).

Mostly exercised reaction or preventive mechanism is filtering or dropping of packets. This method can only handle limited number of packets beyond which the filtering mechanism reaches the deadlock state. According to the recent statistics the amount of packets that arrive during the DDoS attacks are too heavy for any filtering technique to withstand (Kompella *et al*., 2007). Therefore a cooperative filtering mechanism has been introduced in (Hwang *et al*., 2004), this gives the opportunity to the victim server to borrow the packet filters for the situation where a DDoS attack cannot be filtered single handedly.

The next reaction method used noticeably is traceback; it is the existing technology to traceback the attacking sources. Mostly traceback is performed after the attack i.e., Offline (Mirkovic and Reiher, 2005) therefore the traceback mechanism does not prevent the victim from damage.

2.2. Economical Aspect

Most of the cases researchers strive hard in the technical aspect by ignoring the economical aspect, which is the prima facie of DDoS attack, because in every case of DDoS attack the main motive behind is to inflict monetary loss on the victim. All who have faced DDoS attack has lost millions and millions of bucks. The victims around the World are commercial sites, educational institutions, public chat servers, government organizations, financial institutions.

Filtering of packets doesn't make any sense to the zombie, because zombie's doesn't even know about its state of being accomplice. Therefore the zombies keep on flooding the genuine looking packets by obeying the attackers command.

Despite the growth and severity of DDoS attack, victims don't have any mechanism to discourage the zombies from its participation. Moreover the victim is responsible to quell the DDoS attack and to ensure service to their legitimate clients.

Moreover the traceback becomes a daunting task if performed online. The reason is the heavy influx that doesn't allow the traceback mechanism to reach the attacker. If and only if a considerable amount of flood is subsided then only it is possible to perform online traceback effectively (Hwang *et al*., 2004).

Therefore a tchno-economical method termed as penalty scheme is introduced in this study. This method aims at recovering zombie from the Botnet or Decoy net, to mitigate the DDoS attack. It has the benefit of eliminating considerable number of zombies from the Botnet which reduces traffic overhead and creates enough room for online traceback. However to implement the penalty scheme only a simple adjustment should be made in the packet filters.

2.3. Penalty Scheme Execution

The Penalty approach capitalizes on the fact that making the accomplice accountable will deter their future involvement and subsidizes the formidable traffic generated through them. Penalty is the idea for recovering zombie. Penalty is added dynamically at the very moment the Intrusion Detection System (IDS) mechanism detects the DDoS attack. Existing detection techniques can be used to detect the DDoS attack. If and only if it is smart enough to detect DDoS attack at its initial stage (when there is no congestion) and also it should be smart enough to segregate false negative from false positive (Claffy *et al*., 2007). As long as the existing detection techniques segregate the attack traffic cleverly, legitimate users will not be penalized. Moreover Penalty is initiated from the victim based on the attack in the traffic. In case of congestion based DDoS attack penalty can be invoked by intermediate network entities too. However the modern attackers don't allow the flood to cause congestion in the network instead they utilize the upstream and freely available bandwidth to dumb the packets at the victims end by cleverly traversing the network routers and protection entities like firewall pretending as a benign packets. Therefore the victim should always be watchful to invoke the penalty scheme.

As mentioned in **Fig. 1** the penalizing mechanism by making use of existing packet counting mechanism sets its counter to count the IP packets generated by the zombies. The moment a flow is confirmed for its participation in DDoS attack, the Penalty scheme invokes the exponential growth per packet cost algorithm. For the effective functioning of exponential growth strategy this algorithm describes the Maximum Packet Count (MPC) beyond which the service to the user is cut off.

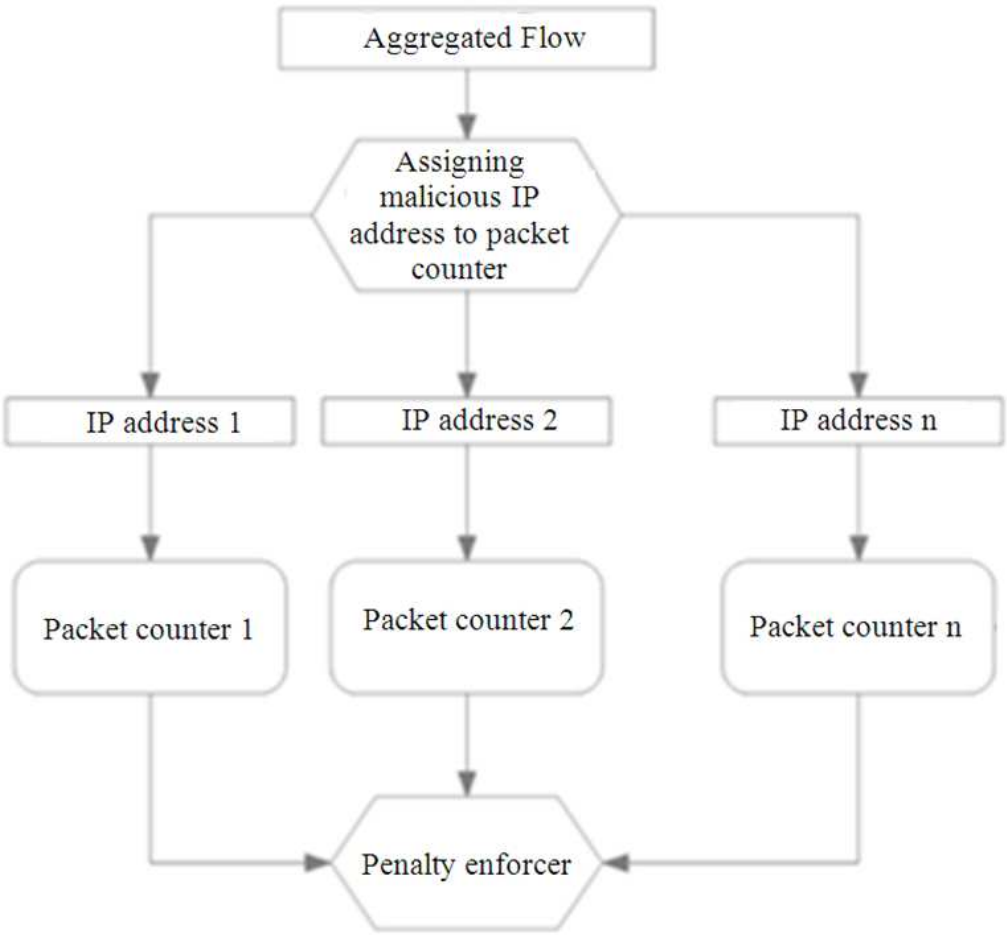

Fig. 1. Work Flow diagram

As given in **Fig. 2** packet counter of penalty algorithm is the counter parallel to the packet counter of filter or any other network entity, initiated only if the traffic shows symptom of DDoS attack. Usual packet counter counts packet always but penalty counter counts only DDoS inflected packets. Using one or more filtering techniques, DDoS traffic even the false negatives are segregated assigned to Penalty packet counter. At the moment the penalty packet counter is invoked, it resets itself to zero and starts counting the packets one by one until the stipulated maximum count reaches. This packet counter is tuned per IP address basis. If 'N' number of IP address participates in the DDoS attack, the mechanism can initiate N packet counters simultaneously but it relies completely on the availability of resources.

Usually the penalty packet counter counts the arriving packet one by one of assigned IP address, the moment the count reaches the Maximum Packet Count (MPC). The exponential growth evaluator or penalty evaluator the single component which receives the packet count and the corresponding IP address from the Packet counter and calculates Penalty for each IP address and forward the penalty to the corresponding IP address along with the attack log (a proof for that particular IP address participation in DDoS attack) to the ISP. After scrutinizing the attack log, ISPs are expected to enforce the penalty and commands connection termination to subscriber whose IP address participated in the attack. After severing the connection ISP should kick start the zombie recovery mechanism by guiding the zombie's to build up a foolproof security. Once the recovery is completed the service is reinstated. The whole process of penalty is given in the following algorithm.

```
While (flow = aggressive)
If (Attack = true);
{Attack_traffic_segregation ();
{Packet_examination()
{If (IP address1 = malicious)
{Int Packet_counter 1= 0;
Assign (Packet_counter1, IP address1)
{For (Packet_counter1 <= MPC ;
Existing_Packet_Counter (count ++); )
//Whenever existing counter counts the packet
// relevant to IP address1 the control transfers here
{Filter(Packet)}
" " "
" " "
If (IP addressN = malicious)
{ int Packet_counter N = 0;
Assign (Packet_counterN, IP addressN)
{For ( Packet_counterN <= MPC;
Existing_Packet_Counter(count++); )
{Filter(Packet)}}
```

Fig. 2. Procedure to assigning n number of packet counters to n number of zombie IP addresses

Technical Algorithm:

Step 1: Detect the DDoS Flow
Step 2: Run the per IP packet counter mechanism to calculate the Penalty
Step 3: Forward the flow details and the log evidence to the Penalty Enforcer
Step 4: Enforce the Penalty scheme which will mitigate the victim resource abuse.
Step 5: Allow blocking, filtering technique, only after calculating penalty.
Step 6: Perform traceback through penalty enforced accomplice.

Financial Algorithm:

However to calculate the penalty following equation is used:

$$P = C (1 + r/n)^{(n + t)}$$

Where:

P = Penalty
r = Number of recorded infected packets (Estimation should have log, should be a constant number)
n = Penalty Index (based on the aggression in the attack) (Approximated Number of packets per second<= 50000 during DDoS attack the penalty index is 2; Approximated Number of packets per second<= 100000 during DDoS attack the penalty index is 4; Approximated Number of packets per second<= 150000 the penalty index is 6)
C = Normal Cost per packets (For pricing scheme other than usage based pricing scheme fix a price based on incremental approach only for this case)
t = (1 + No. of past participation as zombie). [1 stands for the present attack] e.g., C = 0.03$, t = 1, r = 25, n = 2 P = 0.03(1 + 25/2) 2 * 1 = 0.03 (13.5) 2 = 182. 3 *0.03 = 5.5 $.

2.4. Study on Penalty Scheme

In case if a node receives heavy traffic beyond its capability. It may not perform detection, filtering, penalizing and traceback on its own. Instead it may set alarm to cooperative team of filters. The cooperative filters after getting alerted will perform detection, filtering, penalty and trace back. Generally the victim triggers the alarm to other cooperative entities encouraging them to participate in the defense. Those entities may or may not follow the attack path.

Attacker cannot reach the victim without traversing the ISPs. At least local ISPs are outwitted by the attacker to reach the victim. There are two possibilities either ISP is capable of detecting attack by itself. Or else it should be in a position to receive the alarm from the victim of DDoS attack.

Cooperative filtering is a prolific way to forestall the victim from attack especially in case of unbearable aggressive flow. Penalty does not remove packets but it removes the source until it removes the source filtering is required. Filtering here functions as temporary stress reliever requires removing IP packets until the corresponding zombies are taken offline. If the filtering doesn't functions until the completion of penalty scheme, the packets get accumulated in to massive volume. Any productive defense should allow the penalty and filtering function simultaneously i.e. before the IP address is tuned for penalty, filtering is required. In addition, after the IP address is estimated for penalty, until the ISP remove the corresponding source, filtering is necessary.

Penalty can become more forceful if it is integrated with cooperative filters.

Only through penalty the zombie gets the chance to realize that his resource was exploited by an attacker. Acquiring penalty (MPC) from the customer is not the motive behind the penalty scheme, because all the ISPs are at price war (Lin *et al*., 2003) also they are customer conscious they don't want to lose the customers because of penalty. Therefore it is better to withdraw the penalty and exhort the user with contemporary attacks and the necessary preventive measures to be deployed to prevent their resources.

The period from which the service to the customer is repealed after ensuring his active participation as zombie in DDoS attack to the period at which the service is provided back to the zombie is termed as cure period. During this period the security mechanism of zombie is strengthened. Cure period is better if and only if it scales in minutes. If it exceeds hours the payoff may be the loss of customer. So the tradeoff is lesser the cure period provides better retention of customer.

While dividing the traffic among the filters, the traffic from the zombie may be distributed among the filters, say the filter A doesn't listen to the traffic from IP address 1 but the filter B can listen to the traffic from IP address 1. In case of aggregate traffic it is not possible to say that only one filter consistently listens to the traffic from the same IP address. It may listen to the traffic of IP address 1 for a while after that the IP address 1 may assigned to the filter B this may impede the penalty scheme from functioning. Therefore the cooperative filters should be assigned flow specific if it has to incorporate the penalty scheme.

Definitely the entity that has the potential to filter out the traffic will have the tendency to read the IP address of the traffic. Therefore any network entity can calculate the penalty flow specific before filtering the DDoS traffic.

Only ISP to the corresponding zombie are allowed to hold the full right to tear down the subscription and issue the penalty not the other entities. If all the zombies come under the ISP of victim then the effect will be on immediate basis. If not, the victims ISP invite the relevant ISPs to enforce the penalty scheme. Whatever the ways the DDoS attack is defended either with or without cooperative filtering or caching (Kumar *et al*., 2006), enforcing the penalty is possible. In case of cooperative filtering and cooperative caching, the potentiality to estimate the IP address of the packet is crucial to initiate penalty scheme. It is hard for one entity to penalize the entire zombie network. So here we suggest the cooperative penalizing. The reason is the penalty adds small processing over head, if it is shared among various network entities, it will ease the operation.

It is always difficult to penalize the aggregate flow which involves legitimate flow. It is possible for the legitimate being penalized, because the available IDS system may fail to categorize the legitimate traffic from attack traffic. By anticipating such situation, the algorithm provides warning of being penalized during grace period. So the innocent has the chance to go offline at the very moment he receive the warning.

Even if the IDS detects suspicious behaviors in the traffic. The ISP need not deploy penalty immediately. It may refrain for a period called grace period this period can be chosen arbitrarily based on the extent of customer toleration hence to retain the customer. Until the completion of grace period the filters or cooperative filters are used to filter the accumulated traffic.

Setting up of grace period can be indicated to the customer as "You are about to pay penalty because of your participation in Distributed Denial of service attack with or without your knowledge". With this message we can inform the user about him being a zombie. This intimation should reach the customer in the way that it claims his attention. After this period, the DDoS attack mostly involves flow aggression. So the grace period should not exceed the tolerance rate of attack.

A compromised node the zombie if receives penalty the first time, then penalty can be revoked, i.e the only punishment he receives is disconnection from internet service until the attack subsidizes or else until his security is beeped up, He can also be forgotten second time for his participation in DDoS attack, If he receives the penalty for 'N^{th}' time his negligence should be penalized by acquiring the accumulated money from him. This N^{th} time is the intolerance value can be fixed by ISP after mooting with past and possible victims. Considerations should be provided to the zombie in case of DDoS attack that bangs upon inventing new flaws in the software.

3. RESULTS

To perform large scale analysis in real world, the raw data is accumulated from three different dataset providers they are EFNET, QGIS and Eris Free. The datasets contained genuine traffic as well as the DDoS traffic. The DDoS attack flows are segregated from the normal flows by applying various parameters like attack signatures, packet rate per second, invalid, no data and redundant data in payload (Chiueh, 2006).

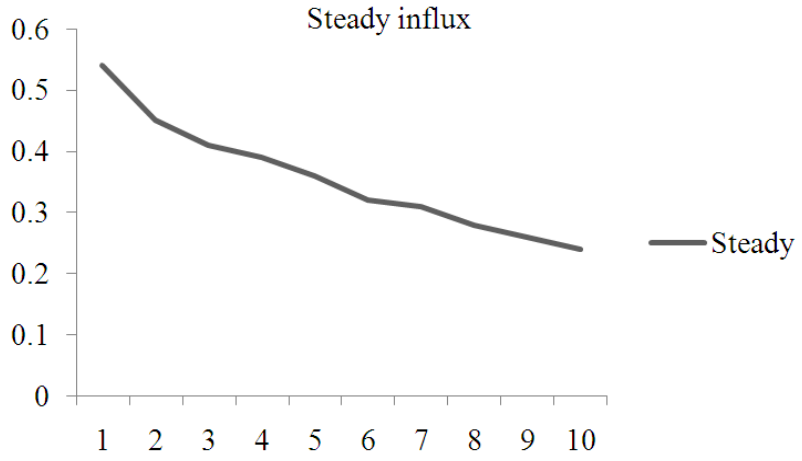

Fig. 3. DDoS attack which maintains constant rate and detected early

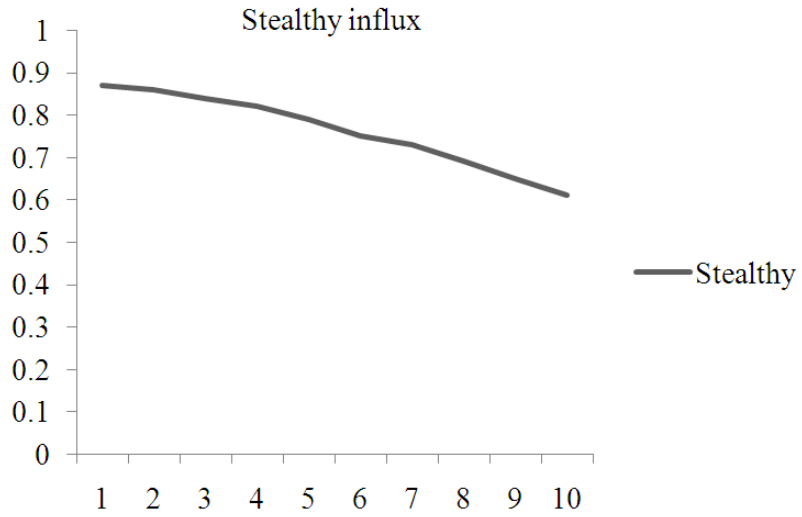

Fig. 4. Penalizing Effects of late detection due to evasive nature of the DDoS Flood

Correlation is then performed to group various DDoS flows based on the similarity in the applied parameters. Moreover analyzing the various DDoS attack attempts they are further classified as steady, stealthy and heavy. However before performing result analysis the following study is performed to find out the probabilistic nature in applying the Penalty algorithm.

Let us consider the number of zombies takes part in the DDoS attack as 'N' When N grows then the condition turns in favor of the attacker. When the N is reduced then the DDoS attack fails to intimidate. If we substitute the value for N in N-1/ N we can estimate the victory factor 'α'. The attacker tries to reach the victory factor by hiring excessive zombies. Consider 1 is the defeat point where the defenders collapse completely, 0 is the point where attackers collapse completely.

The possible way for the defenders to prevent the attacker from gaining the victory point is to remove the zombies from the DDoS attack Network. Existing solution fails mostly because they failed to consider the zombie recovery. As the result the N grows massively and reaches almost 1 to which the defenders does n't withstands and they surrender. Here in our approach we never allow N to grow so the attacker never reaches the victory point. Victory point therefore oscillates between 0 and 1.

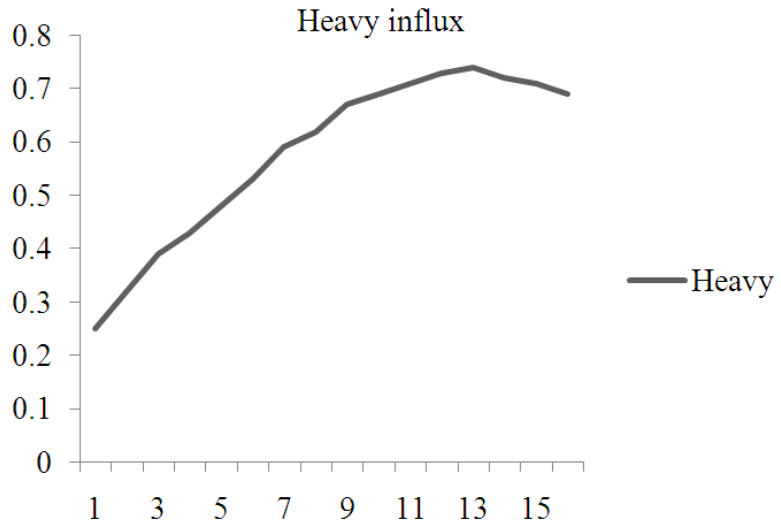

Fig. 5. Penalizing Effects of inundating and heavy DDoS Flood

According to **Fig. 3** if the rate of attack remains constant or near constant. Disconnecting each and every zombie will mitigates the incomming flood drastically.

Accoridng to **Fig. 4** in case of stealthy DDoS influx the attack itself is hard to detect and then segregating the geniune looking attack flows is also a tedious job. Hence disconnecting each and every zombie can only mitigate the incomming flood considerably. However it also removes some flooding source and thus creates enough room to perform online traceback.

Accoridng to **Fig. 5** in case of heavy Influx the rate of attack keeps increasing statically or dynamically. However disconnecting each and every zombie will mitigates the incomming flood considerably to the extent that it can keep the incomming rate handleable by the server.

4. DISCUSSION

4.1. Need for Accurate Detection

If the detection mechanism failed to classify the innocent traffic from the attack traffic there is the possibility for innocent get punished through the penalty.

4.2. Spoofing

Nowadays hackers are keen in hiding their identity but not the identity of the zombies because attackers now have the capability to compromise milions of nodes to perform DDoS attack. Moreover lot of improvement has been made to detect spoofed packets easily, one such is the ingress and egress filtering which is deployed ubiquitously around the Internet.

4.3. Adaptability

The Penalty scheme is not going to rely upon the existing pricing scheme like (Anderson and Moore, 2006) flat rate pricing, usage based pricing, or congestion based pricing scheme (Shakkottai and Srikant, 2006; Jin *et al*., 2005). Therefore Lack of incremental payment structure does not make any difference to penalty. However the idea of penalty scheme is similar to usage based pricing because count of the packets is vital for both the cases, but not the same because penalty is heavier than usage based pricing and invoked dynamically only during the DDoS attack is detected.

4.4. Assistance of Penalty

Without being penalized Zombies allows attacker to avoid getting detected and presumably reduces the attackers bandwidth costs, since the owners of zombies pay for their own bandwidth utilization mindless of the attack traffic flooded through it by the attacker. In such cases penalty creates awareness about paying for traffic generated without the knowledge of the zombie owner. This way one time penalty may avoid subscriber's further compromise for attacker, which indeed eliminate the payment for the traffic doesn't generated by him. ISP by penalizing will have an opportunity to help his customers by suggesting the necessary preventive measures to resist further attacks. If attackers are unable to break into and make use of secondary victim systems (zombies), then the attackers will never form the DDoS attack network from where to launch DDoS attacks.

4.5. Online Traceback

Penalty scheme aims at disconnecting the zombies from the attack the disconnected zombie does not create upstream traffic so performing traceback through the disconnected zombie becomes the easy and quick option. This way Penalty Scheme creates enough room to perform traceback online. Which if implemented may provide enough room for tracing the attacker and helps the victim to withstand the attack.

4.6. Traceback Assistance

Penalty creates the possibility for ISP to track down the attacker through the recovered zombie, by pretending the recovered zombie as the zombie. This will provide more chance for the ISP to track the clever attackers.

5. CONCLUSION

In this study we discussed a brand new scheme called penalty by exponential growth that strives to mutilate DDoS attack through zombie recovery. The strength of the DDoS attack relies on the number of participating zombies. Consequently from the performed analysis the proposed Penalty Scheme deteriorate the DDoS attack by revoking the zombies successively from the Botnet or Decoy network. Thus the effects of DDoS can be mitigated effectively through integrating the Penalty Scheme.

6. REFERENCES

Akella, A., A. Bharambe, M. Reiter and S. Seshan, 2004. Detecting DDoS attacks on ISP networks. Proceedings of the 22nd ACM SIGMOD/PODS Workshop on Management and Processing of Data Streams, (WMPDS' 04).

Anderson, R. and T. Moore, 2006. The economics of information security. Science, 314: 610-613. DOI: 10.1126/science.1130992

Chiueh, S.L.T., 2006. A survey on solutions to distributed denial of service attacks. RPE Report.

Claffy, K., S.O. Bradner and S.D. Meinrath, 2007. The (un)Economic Internet? IEEE Internet Comput., 11: 53-58. 10.1109/MIC.2007.72

Gupta, B.B., R.C. Joshi and M. Misra, 2011. Prediction of number of zombies in a DDoS attack using polynomial regression model. J. Adv. Inform. Technol., 2: 57-62.

Hwang, K., H. Liu and Y. Chen, 2004. Cooperative anomaly and intrusion detection for alert correlation in networked computing systems. IEEE Trans. Dependable Secure Comput.

Jin, N., G. Venkitachalam and S. Jordan, 2005. Dynamic congestion-based pricing of bandwidth and buffer. IEEE/ACM Trans. Network., 13: 1233-1246. DOI: 10.1109/TNET.2005.861252

Kompella, R.R., S. Singh and G. Varghese, 2007. On scalable attack detection in the network. IEEE/ACM Trans. Network., 15: 14-25. DOI: 10.1109/TNET.2006.890115

Kumar, K., R.C. Joshi and K. Singh, 2006. An integrated approach for defending against Distributed Denial-of-Service (DDoS) attacks. IRISS.

Lin, M.H., C.C. Lo and W. Zhuang, 2003. A flexible time-based pricing policy for charging internet services. CAiSE Short Paper Proc.

Mirkovic, J. and P. Reiher, 2005. D-WARD: A source-end defense against flooding denial-of-service attacks. IEEE Trans. Dependable Secure Comput., 2: 216-232.

Oikonomou, G., J. Mirkovic, P. Reiher and M. Robinson. 2006. A framework for a collaborative DDoS defense. Proceedings of the 22nd Annual Computer Security Applications Conference, (ACSAC' 22), IEEE Xplore Press, Miami Beach, FL., pp: 33-42. DOI: 10.1109/ACSAC.2006.5

Shakkottai, S. and R. Srikant, 2006. Economics of network pricing with multiple ISPs. IEEE/ACM Trans. Network., 14: 1233-2145. DOI: 10.1109/TNET.2006.886393

Wang, H., C. Jin and K.G. Shin, 2007. Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Trans. Network., 15: 40-53. DOI: 10.1109/TNET.2006.890133