TRACING DDoS ATTACKS USING ENTROPY VARIATIONS

Ezhilarasi.S
Department of Computer and Communication Engineering, Pavendar Barathidasan College of Engineering and Technology, Trichy

Abstract
Distributed Denial-of-Service (DDoS) attacks are a critical threat to the Internet which deny normal service and degrade quality of service. However, the Network security mechanisms does not have effective and efficient methods to trace back the source of these attacks. In this paper, I propose a novel traceback method for DDoS attacks that is based on entropy variations between normal and DDoS attack traffic, which is fundamentally different from commonly used packet marking techniques. In comparison to the existing DDoS traceback methods, the proposed strategy possesses a number of advantages—it is memory non-intensive, efficiently scalable, robust against packet pollution, and independent of attack traffic patterns. The results are presented to demonstrate the effectiveness and efficiency of the proposed method. My experiment shows that accurate traceback is possible within 20 seconds (approximately) in a large-scale attack network with thousands of zombies and to block them by IP traceback algorithm. The total trace back time is evaluated by monitoring and recording flow information and providing authentication to the new user.

Keywords—DDoS, IP traceback, entropy variation, flow.

Introduction
It is an extraordinary challenge to traceback the source of Distributed Denial-of-Service (DDoS) attacks in the Internet. In DDoS attacks, attackers generate a huge amount of requests to victims through compromised computers (zombies), with the aim of denying normal service or degrading of the quality of services. It has been a major threat to the Internet since year 2000, and a recent survey on the largest 70 Internet operators in the world demonstrated that DDoS attacks are increasing dramatically, and individual attacks are more strong and sophisticated. Furthermore, the survey [1] also found that the peak of 40 gigabit DDoS attacks nearly doubled in 2008 compared with the previous year.

The key reason behind this phenomena is that the network security community does not have effective and efficient traceback methods to locate attackers as it is easy for attackers to disguise themselves by taking advantages of the vulnerabilities of the World Wide Web, such as the dynamic, stateless, and anonymous nature of the Internet[2][3]. IP traceback means the capability of identifying the actual source of any packet sent across the Internet. Because of the vulnerability of the original design of the Internet, we may not be able to find the actual hackers at present. In fact, IP traceback schemes are considered successful if they can identify the zombies from which the DDoS attack packets entered the Internet. Research on DDoS detection [4][5][6], mitigation [8][9], and filtering [10] has been conducted pervasively. However, the efforts on IP traceback are limited. A number of IP traceback approaches have been suggested to identify attackers , and there are two major methods for IP traceback, the probabilistic packet marking (PPM)[12][13] , and the deterministic packet marking (DPM) [14][15][16]. Both of these strategies require routers to inject marks into individual packets. Moreover, the PPM strategy can only operate in a local range of the Internet (ISP network), where the defender has the authority to manage. However, this kind of ISP networks is generally quite small, and we cannot traceback to the attack sources located out of the ISP network.

The DPM strategy requires all the Internet routers [11] to be updated for packet marking. However, with only 25 spare bits available in as IP packet, the scalability of DPM is a huge problem . Moreover, the DPM mechanism poses an extraordinary challenge on storage for packet logging for routers. Therefore, it is infeasible in practice at present. Further, both PPM and DPM are vulnerable to hacking , which is referred to as packet pollution. IP traceback methods should be independent of packet pollution and various attack patterns Entropy rate, the entropy growth rate as the length of a stochastic sequence increases, was employed to find the similarity between normal and attack flows on the entropy growth pattern , and relative entropy, an abstract distance between two probabilistic mass distributions , was taken to measure the instant difference between two flows.

In this paper, I propose a novel mechanism for IP traceback using information theoretical parameters, and there is no packet marking in the proposed strategy; therefore, can avoid the inherited shortcomings of the packet marking mechanisms.

I categorize packets that are passing through a router into flows, which are defined by the upstream router where a packet came from, and the destination address of the packet.

During nonattack periods, routers are required to observe and record entropy variations of local flows. In this paper, I use flow entropy variation or entropy variation interchangeably. Once a DDoS attack has been identified, the victim initiates the following pushback process to identify the locations of zombies: the victim first identifies which of its upstream routers are in the attack tree based on the flow entropy variations it has accumulated, and then submits requests to the related immediate upstream routers. The upstream routers identify where the attack flows came from based on their local entropy variations that they have monitored. Once the immediate upstream routers have identified the attack flows, they will forward the requests to their immediate upstream routers, respectively, to identify...
the attacker sources further; this procedure is repeated in a parallel and distributed fashion until it reaches the attack source(s) or the discrimination limit between attack flows and legitimate flows is satisfied. My analysis, experiments, and simulations demonstrate that the proposed traceback mechanism is effective and efficient compared with the existing methods. In particular, it possesses the following advantages:

- The proposed strategy is fundamentally different from the existing PPM or DPM traceback mechanisms, and it outperforms the available PPM and DPM methods. Because of this essential change, the proposed strategy overcomes the inherited drawbacks of packet marking methods, such as limited scalability, huge demands on storage space, and vulnerability to packet pollutions. The implementation of the proposed method brings no modifications on current routing software. Both PPM and DPM require update on the existing routing software, which is extremely hard to achieve on the Internet. On the other hand, my proposed method can work independently as an additional module on routers for monitoring and recording flow information, and communicating with its upstream and downstream routers when the pushback procedure is carried out.

- The proposed method will be effective for future packet flooding DDoS attacks because it is independent of traffic patterns. Some previous works depend heavily on traffic patterns to conduct their traceback. For example, they expected that traffic patterns obey Poisson distribution or Normal distribution. However, traffic patterns have no impact on the proposed scheme; therefore, we can deal with any complicated attack patterns, even legitimate traffic pattern mimicking attacks.

- The proposed method can archive real-time traceback of attackers. Once the short-term flow information is in place at routers, and the victim notices that it is under attack, it will start the traceback procedure. The workload of traceback is distributed, and the overall traceback time mainly depends on the network delays between the victim and the attackers.

Background and related work

Background of ddos attacks

DDoS attacks are targeted at exhausting the victim’s resources, such as network bandwidth, computing power, and operating system data structures. To launch a DDoS attack, the attacker(s) first establishes a network of computers that will be used to generate the huge volume of traffic needed to deny services to legitimate users of the victim. To create this attack network, attackers discover vulnerable hosts on the network. Vulnerable hosts are those that are either running no antivirus or out-of-date antivirus software, or those that have not been properly patched. These are exploited by the attackers who use the vulnerability to gain access to these hosts.

The next step for the attacker is to install new programs (known as attack tools) on the compromised hosts of the attack network. The hosts running these attack tools are known as zombies, and they can be used to carry out any attack under the control of the attacker. Numerous zombies together form an army or botnet. There are two categories of DDoS attacks, typical DDoS attacks and Distributed Reflection Denial-of-Service (DRDoS) attacks. In a typical DDoS attack, the master computer orders the zombies to run the attack tools to send huge volume of packets to the victim, to exhaust the victim’s resources. Unlike the typical DDoS attacks, the army of a DRDoS attack consists of master zombies, slave zombies, and reflectors. The difference in this type of attack is that slave zombies are led by master zombies to send a stream of packets with the victim’s IP address as the source IP address to other uninfected machines (known as reflectors), exhorting these machines to connect with the victim. Then the reflectors send the victim a great volume of traffic, as a reply to its exhortation for the opening of a new connection, because they believe that the victim was the host that asked for it. Understanding the features of DDoS attack is critical for effective attack traceback. However, we have limited real data sets about DDoS attacks. The current knowledge of DDoS attack can be classified as follows: inference based on partial information, real network emulation or simulations, and real attack and defence between two cooperate research groups.

Related Work of IP Traceback

Packet marking methods include the PPM and the DPM. The PPM mechanism tries to mark packets with the router’s IP address information by probability on the local router, and the victim can reconstruct the paths that the attack packets went through. The PPM method is vulnerable to attackers, as attackers can send spoofed marking information to the victim to mislead the victim. The accuracy of PPM is another problem because the marked messages by the routers who are closer to the leaves (which means far away from the victim) could be overwritten by the downstream routers on the attack tree. At the same time, most of the PPM algorithms suffer from the storage space problem to store large amount of marked packets for reconstructing the attack tree. Moreover, PPM requires all the Internet routers to be involved in marking.

Based on the PPM mechanism, tried to traceback the attackers using traffic rates of packets, which were targeted on the victim. The model bears a very strong assumption: the traffic pattern has to obey the Poisson distribution, which is not always true in the Internet. Moreover, it inherits the disadvantages of the PPM mechanism: large amount of marked packets are expected to reconstruct the attack diagram, centralized processing on the victim, and it is easy be fooled by attackers using packet pollution.

The deterministic packet marking mechanism tries to mark the spare space of a packet with the packet’s initial router’s information, e.g., IP address. Therefore, the receiver can identify the source location of the packets once it has sufficient information of the marks. The major problem of DPM is that it involves modifications of the current routing software, and it may require very large amount of marks for packet reconstruction. Moreover, similar
to PPM, the DPM mechanism cannot avoid pollution from attackers.

System modeling for ip traceback on entropy variations

A Sample Network with ddos Attacks

In order to clearly describe my traceback mechanism, I use Fig. 1 as a sample network with DDoS attacks to demonstrate our traceback strategy. In a DDoS attack scenario, as shown in Fig. 1, the flows with destination as the victim include legitimate flows, such as f3, and a combination of attack flows and legitimate flows, such as f1 and f2. Compared with nonattack cases, the volumes of some flows increase significantly in a very short time period in DDoS attack cases. Observers at routers R1, R4, R5, and V will notice the dramatic changes; however, the routers who are not in the attack paths, such as R2 and R3, will not be able to sense the variations. Therefore, once the victim realizes an ongoing attack, it can pushback to the LANs, which caused the changes based on the information of flow entropy variations, and therefore, we can identify the locations of attackers.

The traceback can be done in a parallel and distributed fashion in our proposed scheme, based on its knowledge of entropy variations, the victim knows that attackers are somewhere behind router R1, and no attackers are behind router R2. Then the traceback request is delivered to router R1. Similar to the victim, router R1 knows that there are two groups of attackers, one group is behind the link to LAN0 and another group is behind the link to LAN1. Then the traceback requests are further delivered to the edge routers of LAN0 and LAN1, respectively. Based on entropy variation information of router R3, the edge router of LAN0 can infer that the attackers are located in the local area network, LAN0. Similarly, the edge router of LAN1 finds that there are attackers in LAN1; furthermore, there are attackers behind router R4. The traceback request is then further passed to the upstream routers, until we locate the attackers in LAN5.

System Modelling

In this paper, I categorize the packets that are passing through a router into flows. A flow is defined by a pair—the upstream router where the packet came from, and the destination address of the packet. Entropy is an information theoretic concept, which is a measure of randomness. I employ entropy variation in this paper to measure changes of randomness of flows at a router for a given time interval. We notice that entropy variation is only one of the possible metrics however, attackers could cheat this feature by increasing attack strength slowly. We can also employ other statistic metrics to measure the randomness, such as standard variation or high-order moments of flows. We choose entropy variation rather than others in this paper because of the low computing workload for entropy variations.

In this section, I first compare the proposed model with the existing proposals in order to show the advantages of the proposed mechanism. I then analyze the proposed entropy-variation-based traceback model in detail. The features of a stand-alone router are analyzed first, followed by the investigation on the properties of the whole attack tree of a DDoS attack.

Comparison of Traceback Models

In order to show the advantages of the proposed mechanism, we compare our proposed method with the representatives of DPM and PPM algorithms.

Analysis of Entropy-Variation-Based Traceback Model

I present my assumptions below in order to make my analysis simple and clear. We assume the following:
1. There is no extraordinary change of network traffic a very short time interval (e.g., at the level of seconds) for non-DDoS attack cases. It is true that the network traffic for a router may dynamically change a lot from peak to off-peak service times. However, this kind of change lasts for a relatively long time interval, e.g., at least at the level of minutes. If we break down these changes into seconds, the change of traffic is quite smooth in our context.
2. The number of attack packets is at least an order of magnitude higher than that of normal flows. During a DDoS flooding attack, the number of attack packets increases dramatically, and the attack packets are generated by thousands of zombies or bots. Consequently, the number of attack packets is much higher than that of legitimate flows. Therefore, this assumption is reasonable. Of course, for the nonflooding attacks, this may not hold, and in this paper, we focus on the majority of the attack tools—flooding attacks. Furthermore, this is the lower bound that we can discriminate attack flows from the legitimate flows.
3. Only one DDoS attack is ongoing at a given time. It could be true that a number of attacks are ongoing concurrently in the Internet, the attack paths
may overlap as well, but we only consider the one attack scenario to make it simple and clear.

4. The number of flows for a given router is stable at both the attack cases and nonattack cases.

Compared with the nonattack scenario, the upper bound of entropy variation drops when DDoS attack flows are passing through a local router. For a local router on an attack path, the entropy variation of the output flows is not greater than the summation of the entropy variation of the incoming flows. Compared with the nonattack situation, the entropy variation of a local router drops dramatically when attack flows are passing through the local router. The entropy variation drops when a local router is closer to the victim, and vice versa.

Based on the partial information of the attack that the traceback algorithm has accumulated, we can estimate the number of zombies to be traced and the maximum length to the most far away zombie(s). There are no attackers at the upstream routers if a local router’s entropy variation is reasonable.

**ALGORITHMS FOR THE IP TRACEBACK MODEL**

In this section, we design the related algorithms according to our previous modeling and analysis. There are two algorithms in the proposed traceback suite, the local flow monitoring algorithm and the IP traceback algorithm. The local flow monitoring algorithm is running at the nonattack period, accumulating information from normal network flows, and progressing the mean and the standard variation of flows. The progressing suspends when a DDoS attack is ongoing. Once a DDoS attack has been confirmed by any of the existing DDoS detection algorithms, then the victim starts the IP traceback algorithm.

The IP traceback algorithm is installed at routers. It is initiated by the victim, and at the upstream routers, it is triggered by the IP traceback requests from the victim or the downstream routers which are on the attack path. The proposed algorithms are independent from the current routing software, they can work as independent modules at routers. As a result, we do not need to change the current routing software.

**TABLE 1: The Comparison of the Entropy Variation Mechanisms against DPM and PPM**

<table>
<thead>
<tr>
<th></th>
<th>DPM</th>
<th>PPM</th>
<th>Entropy Variation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability</td>
<td>High</td>
<td>Low</td>
<td>Very High</td>
</tr>
<tr>
<td></td>
<td>$2^{n}$ computers for single packet marking, more or multiple packet marking</td>
<td>100 routers range of attack tree</td>
<td>Unlimited under condition that every zombie generates obvious traffic</td>
</tr>
<tr>
<td>Storage</td>
<td>High</td>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td></td>
<td>3.3G-44G/minute at each involved router</td>
<td>Around 900M at the victim for one attack</td>
<td>24Gk/minute at involved routers</td>
</tr>
<tr>
<td>Traceback Time</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Network delay</td>
<td>Network delay plus calculation time</td>
<td>Network delay</td>
</tr>
<tr>
<td>Operation Workload</td>
<td>High</td>
<td>Very High</td>
<td>Very Low</td>
</tr>
<tr>
<td></td>
<td>Digesting packets with probability $P$ (about 1M packets/second)</td>
<td>Marking packets with probability $P$ (about 1M packets/second)</td>
<td>Counting packet numbers for each flow</td>
</tr>
</tbody>
</table>
Conclusion
In this paper, I proposed an effective and efficient IP traceback scheme against DDoS attacks based on entropy variations. It is a fundamentally different traceback mechanism from the currently adopted packet marking strategies. Many of the available work on IP traceback depend on packet marking, either probabilistic packet marking or deterministic packet marking. Because of the vulnerability of the Internet, the packet marking mechanism suffers a number of serious drawbacks: lack of scalability; vulnerability to packet pollution from hackers and extraordinary challenge on storage space at victims or intermediate routers. On the other hand, the proposed method needs no marking on packets, and therefore, avoids the inherent shortcomings of packet marking mechanisms.

It employs the features that are out of the control of hackers to conduct IP traceback. We observe and store short-term information of flow entropy variations at routers. Once a DDoS attack has been identified by the victim via detection algorithms, the victim then initiates the pushback tracing procedure. The traceback algorithm first identifies its upstream routers where the attack flows came from, and then submits the traceback requests to the related upstream routers. This procedure continues until the most far away zombies are identified or when it reaches the discrimination limitation of DDoS attack flows. Extensive experiments and simulations have been conducted, and the results demonstrate that the proposed mechanism works very well in terms of effectiveness and efficiency. Compared with previous works, the proposed strategy can traceback fast in larger scale attack networks. It can traceback to the most far away zombies within 20 seconds in the worst case under the condition of thousands of zombies. Moreover, the proposed model can work as an independent software module with current routing software. This makes it a feasible and easy to be implemented solution for the current Internet.

FUTURE WORK
Future work could be carried out in the following promising directions:
1. The metric for DDoS attack flows could be further explored. The proposed method deals with the packet flooding type of attacks perfectly. However, for the attacks with small number attack packet rates, therefore, a metric of finer granularity is required.
2. Location estimation of attackers with partial information.
3. Differentiation of the DDoS attacks and flash crowds. In this paper, we did not consider this issue—them proposed method may treat flash crowd as a DDoS attack.

References