INVITED PAPER *Special Section on Information and Communication System Security*

Overview of Traceback Mechanisms and Their Applicability

Heung-Youl YOUM[†a)], ***Nonmember***

SUMMARY As an increasing number of businesses and services depend on the Internet, protecting them against DDoS (Distributed Denial of Service) attacks becomes a critical issue. A traceback is used to discover technical information concerning the ingress points, paths, partial paths or sources of a packet or packets causing a problematic network event. The traceback mechanism is a useful tool to identify the attack source of the (DDoS) attack, which ultimately leads to preventing against the DDoS attack. There are numerous traceback mechanisms that have been proposed by many researchers. In this paper, we analyze the existing traceback mechanisms, describe the common security capabilities of traceback mechanisms, and evaluate them in terms of the various criteria. In addition, we identify typical application of traceback mechanisms.

key words: *traceback, packet logging, packet marking, overlay network, hybrid traceback, denial of service*

1. Introduction

As an increasing number of businesses and services depend on the Internet, protecting them against DDoS (Distributed Denial of Service) attacks becomes a critical issue. The DDoS attacks have happened frequently since 2005 when cyber crimes for the purpose of monetary gains skyrocketed. Their main targets have been web portals, online shopping sites and websites of financial institutions, as a means of extorting money. Especially, massive DDoS attacks happened twice in South Korea: the 7.7 DDoS attack launched on July 7, 2009 and the 3.4 DDoS attack that launched on March 4, 2011 [1]–[3]. There were two most distinguishing features of these DDoS attacks: unclear purpose of attacks and that around hundred thousand malware-infected computers being used to launch these attacks. In addition, taking into account that some critical infrastructures service are increasingly relying on the Internet, they are required to have effective countermeasures against DDoS attacks.

One of the challenges for preventing against DDoS attacks is that attackers mostly use spoofed source IP addresses (hereafter referred to as spoofed IP addresses) which make it difficult for network administrators to identify and block the attack packets used on the Internet. In order to solve the DDoS problems, many researchers have proposed traceback techniques. It is agreed that one of most practical ways is to use a traceback mechanism to identify the source of attackers by marking, logging information on packets by the router residing on the attack path or route them to specific point to investigate the attack packet. This mechanism may allow victims or network operators to reconstruct the path that the packets take from the source of attacker through the Internet, despite hacker uses spoofed IP address.

We use term on a traceback as techniques used to discover technical information concerning the ingress points, paths, partial paths or sources of a packet or packets causing a problematic network event, generally for the purposes of applying mitigation measures defined in [13]. In fact, to achieve this goal, it needs a technical and/or administrative process for reliably identifying the source of IP packet or IP packets which may or may not be spoofed by the sender or the paths or part of paths which are used for attacks by the attacker. A traceback mechanism is a specific mechanism that is used to identify the hacker's physical and logical location in real time with the help of network elements such as router or the hosts in the network when the attacks take place in the network.

This paper focuses presenting taxonomy, a survey of prominent traceback techniques, global standardization activities of IP traceback techniques, evaluation criteria, and a comparison in terms of evaluation criteria.

The rest of the paper is organized as follows. In Sect. 2, we present the taxonomy of traceback mechanisms and capabilities that some traceback mechanisms may have. In Sect. 3, we present the analysis of the existing well-known traceback mechanisms and evaluate them in terms of critical evaluation criteria. In Sect. 4, we explore typical application of traceback mechanisms. Finally, we conclude this paper in Sect. 5.

2. Taxonomy and Capabilities

2.1 Taxonomy of Traceback Mechanisms

There have been taxonomies and surveys of traceback mechanisms in [4]–[12]. An Autonomous System (AS) is defined as a collection of IP networks and routers under the control of one entity that presents a common, clearly defined routing policy to the Internet. The taxonomy of IP traceback mechanisms shown in Table 1 is the slightly modified one proposed in [4].

The IP traceback mechanisms are classified into Intra-AS traceback and Inter-AS traceback from the viewpoint of the administrative domain. The former assumes that the entire network is under control while the latter assume that an AS may consist of different administrative policies on

Manuscript received May 27, 2011.

[†]The author is with the Faculty of the Department of Information Security Engineering, Soonchunhyang University, Korea.

a) E-mail: hyyoum@sch.ac.kr

DOI: 10.1587/transinf.E94.D.2077

Table 1 Taxonomy of IP traceback mechanisms.

Categories			Description of basic operation	Example of mechanism
Intra-AS Traceback	Traffic Monitoring	controlled flooding	Apply controlled intentional traffic and identify the links used for attack.	[17]
		Input debugging	Investigate packet based on a packet digest or a signature to identify the link used for attack.	[16]
	Packet Monitoring	Overlay network	All packets are forwarded to a specific network point for inspection.	[18]–[21]
		Packet marking	The routers insert information into some part of the IP header.	[22]–[38]
		Packet Messaging	The routers residing on the attack path send special packet containing traceback information to the victims.	[39]–[41]
		Packet logging	The router logs packets at routers and check whether specific packets have traversed the routers	[42]–[47]
		Hybrid	The routers mark packets with router's IP address or sends special packets while logging packets.	[48]–[50]
Inter-AS traceback			Traceback information should be exchanged between different autonomous systems each of which implements different traceback mechanism for its networks	[52]–[56]

traceback system implementation. Note that the any Intra-AS traceback mechanism can be used as a building block to construct an Inter-AS traceback mechanism. That is, some of inter-AS traceback mechanisms may be used to construct as a building block the Inter-AS traceback systems without much significant modification.

The Intra-AS traceback mechanisms are further classified into Traffic Monitoring type and Packet Monitoring type from the viewpoint of the target of analysis. The former analyzes the traffic/stream of an attack while the latter analyzes each packet.

The Traffic Monitoring type is classified into Controlled Flooding type and input debugging type. The former controls traffic amount, detects anomalies and traces the attack source while the latter analyzes traffic pattern, identifies anomalies and traces the attack source.

The Packet Monitoring type is further classified into Packet Marking type, Messaging type, Packet Logging type, Hybrid type and Overlay type from the viewpoint of routers' behaviors. The Packet Marking type modifies, appends, and/or encapsulates packets at routers in order to mark them. The modified packets are analyzed at the host node that is usually a victim. The Packet Messaging type sends messages from routers to victims, be it either deterministically or probabilistically. The Packet Logging type stores audit logs of forwarded packets at routers. This type is designed to identify the true source of even a single particular IP packet, and require the intermediate routers to log the passage of IP packets. The Hybrid type selectively does either storing audit logs of forwarded packets, marking packets, or sending messages. The overlay type reroutes the packets to a specific network point where they are inspected to identify the attack source.

2.2 Capabilities of Traceback Mechnism

Most existing traceback mechanisms are to identify an attack sources or part of the attack path in [13] as follows;

- Source identification by a service provider:
  A service provider seeking to uncover the source of a problematic network event may use traceback immediately after the incident has been identified. In the scenario in which the service provider has made appropriate investment in and configuration of core routers and edge routers, operators may be able to uncover at the edge router or the incoming physical port, the source of the problematic network event. Source identification may help operators stop or mitigate the impact of the problematic network event.
- Ingress point identification within a region/domain:
  A region/domain, having multiple links to adjacent regions/domains, may use traceback to identify the set of affected links from a particular network incident. The ability to narrow down the number of affected links may help operators expedite the investigation and, when necessary, mitigation procedures.
- Partial path identification across multiple regions/domains:
  If traceback is possible across multiple regions/domains, they can be used to uncover a partial path of widespread attacks. While source identification across multiple regions/domains may be difficult under partial deployment, some traceback may be able to identify the partial path or multiple paths of problematic network event, thus helping mitigation procedures across multiple regions/domains.

2.3 Standard Activities in ITU-T SG17

The first proposal to study IP-traceback techniques emerged at the ITU-T SG 17 April 2007 meeting in the form of a tutorial presentation by one of the Study Group's Vice-chairs. As of May 2011, there are three draft Recommendations for the traceback under development by the Question 4 (cyber-

Table 2 ITU-T standardization activities.

Recommendations/Title	Title/Abstract	Document Status
ITU-T X.rid : Real-time inter-network defense [15]	Real-time inter-network defense (RID) provides a framework for the exchange of incident information. The RID Recommendation provides the set of incident coordination message necessary to communicate IODEF documents securely between entities. RID is essentially a wrapper for IODEF documents, including any extensions of IODEF. The standard messages and exchange formats include security, privacy and policy options/considerations that are necessary in a global incident coordination scheme. RID is the security layer between IODEF document and the transport protocol.	Under development
ITU-T X.trm : Overview of traceback mechanisms [14]	This Recommendation describes and compares various types of traceback mechanisms by the criteria described in this Recommendation.	Under development
ITU-T X.1211 (X.tb-ucc) : Usability of network traceback [13]	This Recommendation describes capabilities derived from example traceback use cases. The use cases include traceback scenarios which occur in a single ISP, a single region/domain and across multiple regions/domains.	Under TAP

security) in the ITU-T SG 17: X.tb-ucc, usability of network traceback [13], X.trm, overview of traceback mechanisms [14], and X.rid, real-time interwork defense [15]. The X.tb-ucc was determined at the April 2011 SG 17 meeting, is under the TAP (Traditional Approval Procedure) as of May 2011, and is planned to consider approval at the September 2011 ITU-T SG 17 meeting, if there is no serious comments during TAP procedure by ITU-T members. The summary of those activities is shown in Table 2.

3. Analysis of Existing Traceback Mechanisms

This section describes some prominent existing traceback mechanisms which are operated at the IP layer.

3.1 Traceback Mechanism with Traffic Monitoring

Most of existing traceback mechanisms start from the router closest to the victim and interactively test its upstream links until they determine which one is used to carry the attacker's traffic. Ideally, this procedure is repeated recursively on the upstream router until the source is reached. This technique assumes that an attack remains active until the completion of a trace and is therefore inappropriate for attacks that are detected after the fact, attacks that occur intermittently, or attacks that modulate their behavior in response to a traceback (it is prudent to assume the attacker is fully informed). Though there are traffic monitoring schemes in which a traceback mechanism checks whether or not the link is part of attack path, there are two varieties traffic monitoring schemes, input debugging and controlled flooding.

Controlled flooding works by generating a burst of network traffic from the victim's network to the upstream network segments and observing how this intentionally generated flood affects the incoming attack traffic's intensity [17]. The traceback is conducted by a network administrator who is aware of network topology very well. Using a known network topology around the victim, these packet floods are targeted specifically at certain hosts upstream from the victim's network; they iteratively flood each incoming network link on the routers closest to the victim's network. From drop in the attack traffic's frequency and intensity, the victim can deduce the incoming network link on the upstream router and repeat the same process on the router one level above.

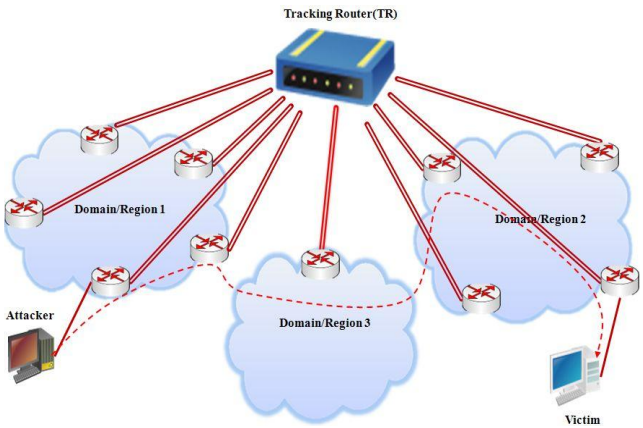

Fig. 1 Concept of overlay network.

Input debugging is one implementation of the link testing mechanism [16]. A feature already exists on many routers. This feature allows the administrator to determine incoming network links for specific packets. If the router is aware of the common characteristics of the attack packets (called the attack signature), then it's possible for the administrator to determine the incoming network link that they arrive on. This is repeated hop-by-hop at every upstream router in the network until the source or another ISP is reached. The obvious problem with the input debugging is its considerable management overhead.

3.2 Traceback Mechanism with Overlay Network

This type of traceback mechanism forwards packets to a certain network point, where they are monitored in the network. It is useful within an ISP domain.

- CenterTrack:
  CenterTrack [18] is an overlay network-based centralized traceback mechanism shown in Fig. 1.
  It introduces a Tracking Router (TR), a special type

of router, which is connected with the edge router physically or virtually with an IP tunnel, called GRE (generic route encapsulation) tunnel, in a network. All TRs should optionally be connected to a central TR via IP tunnels resulting in creating a total overlay network. The star-like topology with the TR and edge router forms an overlay network. When an attack is detected, a victim node sends the traceback relevant information to a TR. The TR uses signature based intrusion detection scheme to identify the source of the attack. The malicious traffic is routed through the overlay network via dynamic routing protocol.

- IP traceback with IPSec:
  This mechanism [19] is based on an assumption that complete network topology is known to the system. The analysis is carried out by setting up IPSec tunnels between an arbitrary router and the victim: If the attack packets detected are authenticated by that association, the attack originates at a point behind this router; if the packets of the attack are not authenticated by this security association, the attack originates in the path between this router and the victim. By establishing these security associations, it is possible for victim to identify the attack source which would be several hops from it. Note that ISP involvement is essential as the knowledge of the network topology is required for each router.
- Black-holing:
  Black-holing mechanism [20], [21] describes an operational technique that utilizes a sinkhole tunnel. A sinkhole tunnel is implemented at all possible entry points from which attacks can pass into the destination / attacked autonomous system. Using the BGP community technique, data traffic destined to the attacked / targeted host could be re-routed to a special path (tunnel) where a sniffer could capture the traffic for analysis. After being analyzed, traffic will exit on the tunnel and be routed normally to the destination host. In other words, the traffic will pass through the network to a sniffer without altering the next hop information of the destination network. All routers within the destination / attacked AS domain will have the proper next hop address. Only the entry point router will have the altered next hop information. Through the analysis, the edge routers within the destination /attacked autonomous system the attack is coming from are revealed. Note that this scheme focuses on DDoS mitigation rather than tracing back to the attack source.

3.3 Traceback Mechanism with Packet Marking

Traceback mechanisms in this category modify, append, and/or encapsulate packets at routers. Those modified packets are analyzed at the host node that is usually a victim node. Major schemes are described below.

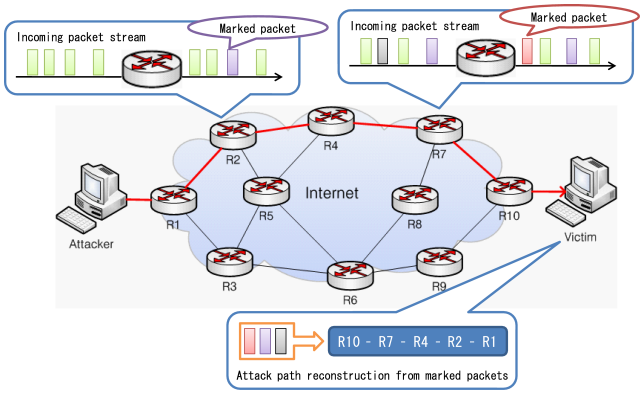

Fig. 2 PPM.

- Probabilistic packet marking:
  The probabilistic packet marking (PPM) mechanism shown in Fig. 2 is characterized by inserting traceback message into the IP packet to be traced, thus marking the packet on its way through the various routers on the network to the destination host [22].
  It uses the 16-bit identification field in the IP header to store a router's address. Packets are marked with the certain probability, for example, 1/25. The marked packet stores information about only one link in the attack path. In other word, PPM is a traceback scheme that inserts router's information in a packet that pass the router along the attack chain so that the victim host can constructs the attack path, even if an attacker uses the spoofed IP address instead of real IP address.

To mark its address, this mechanism should change part of IP header, i.e., the IP identification filed which is used by the AH (authentication header) protocol in the IPsec architecture. In order for the administrator to run this mechanism, it should be assumed that the network should not use AH protocol. Therefore, it can be used within an AS where it does not use the AH protocol.

- Deterministic packet marking (DPM):
  In deterministic marking mechanism, only the ingress router on the attack path marks every packet passing through it with its router IP address [23], enabling a victim to identify packets traversing the same paths through the Internet on a per packet basis, regardless of source IP address spoofing. It also uses the 16-bit identification filed and reserved 1-bit flag field. The IP address is split into two halves of 16 bit each and a randomly chosen segment is marked in the ID filed in the IP header. The 1-bit flag is used to inform the victim which fragment is marked in the ID field, that is, "0" indicates the first half of IP address and "1" indicates the second half of IP address. The merit of this mechanisms is in that s network can implement it without revealing its internal network topology.
- Advanced and authenticated packet marking (AAM):
  This scheme is an enhanced variant of the PPM

scheme [24]. AAM has been designed keeping in mind to avoid the problem of spurious packet markings generated in PPM when a router is compromised. There are two variants proposed: an algorithm for advanced marking, and an algorithm for advanced and authenticated marking scheme. This scheme also uses the 16-bit ID field in the IP header which is split into a 11-bit edge field and 5-bit distance field. In the algorithm for advanced marking scheme, as in PPM, each router marks the packets probabilistically. If a router chooses to mark, each router writes instead of just its address, the hash of its IP address in the 11-bit edge field of IP header and sets the 5-bit distance field to zero. Else, a non-marking router checks if the packet has been already marked by an upstream router. If yes, it overwrites the edge field with the XOR of hash of its IP address with old content and increments the Distance field count. If no, just increment the distance field count. In the algorithm for advanced and authenticated marking scheme, it is assumed each router in the network shares with the victim a secret key Ki and uses message authentication code like HMAC to authenticate the markings of a router. Each router applies HMAC function (rather than a plain hash function) to its IP address in order to authenticate the validity of the markings. Thus, AAM provides strong authentication of router markings. This authenticated marking prevents generation of spoofed marking by any compromised router.

Based on the packet marking, there are several variants of the packet marking techniques that have been proposed by many researchers [25]–[38].

3.4 Traceback with Packet Messaging

The basic idea of traceback with messaging is that each router generates special purpose packets for each packet and writes its IP address in the special packet and forwards them to the destination host. The most prominent scheme is an ICMP traceback.

- ICMP traceback:
  This mechanism determines the full path of the attack shown in Fig. 3.
  In case of ICMP Traceback [39], so called iTrace, as a packet traverses through the network, each router residing in the attack chain probabilistically create a separate trace packet, that is, an ICMP packet for every certain number of packets passing through it on the way to a victim node, i.e., for only one ICMP packet in 20,000 packets. The ICMP packet generated is then forwarded to the victim node. All the gathered ICMP packets are used to determine the attack path to the victim node at the destination node. As there are a flood of packets in the DDoS attacks, it is sufficient for victim to receive a considerable amount of trace packet. The iTrace message itself consists of the next and previous hop information and a time stamp. The iTrace message, an ICMP packet includes the traceback information such as the IP address of a router residing in the attack chain in the ICMP payload. Initial value of TTL (Time To Live) field is set to 255 when creating iTrace message and being transmitted. The Time To Live (TTL) field is then used to identify the actual path depth of the attack. Based on packet messaging, there are some variants proposed: intension-driven iTrace [40] and iCaddie ICMP [41].

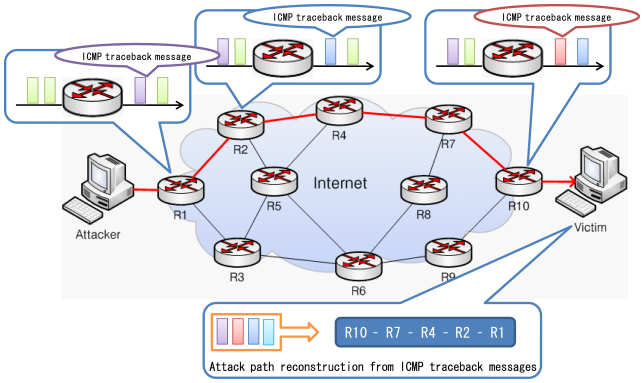

Fig. 3 Concept of iTrace.

3.5 Traceback Mechanism with Packet Logging

The basic idea of traceback with packet logging is that each router logs information (digests or signature of a packet) of all IP packets that traverse through it. Once the attack is detected, the victim queries the upstream routers by checking whether they have logged the attack packet in question or not. If information of attack is found in their memory, then that router is assumed to be part of the attack path. The major problem of logging type traceback is the enormous amount of storage space.

In order to consider the packet transformation, it is based on the invariant portions of 20-byte IPv4 header and the first 8 bytes of payload. Therefore, it uses an invariant portion of the IP header and payload. However, it requires a large amount of memory to store the 28-byte packet information. In order to reduce the storage size, instead of storing the entire 28-byte packet information, hashing is done to it, followed by a Bloom filter processing. By this further refinement, the scheme reduces memory storage requirement in the router to 0.5% of link bandwidth per unit time. It also provides privacy and prevents against eavesdropping of legitimate traffic stream.

- Hash-based IP traceback:
  The scheme is called Source Path Isolation Engine (SPIE) [42], [44]. The basic idea behind the hash-based IP traceback is in that every router captures partial information i.e., invariant portion, of every packet that passes through the router, to be able in the future to determine if that packet passed through it. Each router

computes packet digest f every packet that is captured by a router and stores it using a space-efficient data structure known as Bloom filter [43].
In this scheme such routers are called data generation agents (DGAs). DGA functionality is implemented on the routers. The network is logically divided into regions. In every region SPIE collection and reduction agents (SCARs) connect to all DGAs, and are able to query them for necessary information. The SPIE traceback manager (STM) is a central management unit that communicates to IDSs of the victims and SCARs.
As packets traverse the network, digests of the packets get stored in the DGAs. In this scheme, invariant fields from the IP header and the first 8 bytes of the payload of each packet are hashed by several hash functions to produce several digests. Digests are stored in a space-efficient data structure called a bloom filter, which reduces storage requirements by several orders of magnitude. When a bloom filter reaches at about 70 % full, it is archived for later querying, and another one is used.

Based on packet logging, there are some variants that have been proposed by many researchers [45]–[47].

3.6 Hybrid Traceback Type

The hybrid type combines the Packet Marking type, Messaging type, and Packet Logging type. Although several types of such hybrids are logically available, only the ones of Packet Marking type and Packet Logging type are developed further practically.

- Hybrid mechanisms employing packet marking and logging:
  A hybrid scheme was proposed to record network path information partially at routers and partially in packets [48]. This mechanism introduces the distributed link-list (DLL) concept which is to keep track of a subset of the routers that are involved in forwarding certain packet by establishing a temporary link between them in a distributed manner. The DLL is based on a "store, mark and forward" approach. A fixed-size marking field is allocated in each packet. Any router that decides to mark the packet, stores the current content of the marking field (which was written by the previous marking router) in a special data structure called Marking Table maintained at the router. The router generates an ID for that packet to index its marking information in the marking table. The router marks the packet by overwriting the marking field by its own IP address, and then forwards the packet as usual. Any router that decides not to mark the packet just forwards it.

Based on hybrid traceback mechanisms, there are several variants for hybrid schemes that have been proposed by many researchers [49], [50].

3.7 Inter-AS Traceback

In order to construct global-scale traceback beyond an AS, differing administration policies and regulation among countries and organizations need to be considered. Practically, it is hard to assume that all network domains adopt and deploy a single traceback mechanism. Moreover, some AS may wish to conceal detailed information about traceback mechanism that is deployed. Inter-AS traceback mechanisms can be used to address these issues. Inter-AS traceback uses the communication between Autonomous systems and may allow them to implement arbitrary traceback mechanisms based on the policies. With this type of mechanisms, all different network operators may not implement a single traceback mechanism on all the routers provided one representative router implement the Inter-AS traceback scheme, and the their own traceback mechanisms are implemented to conceal information about this traceback of outside.

- AS-level single packet traceback:
  Korkmaz and Gong et al. combined SPIE mechanisms and the concept of AS SPIE. In this mechanism, an AS-level Single Packet Traceback (AS-SPT) was proposed to facilitate global deployment [51]. The scheme utilizes BGP attribute to understand the network topology. When a victim wants to trace the attack path back to the attack source, it sends inquiries to the routers implementing the traceback mechanism level-by-level.
  For the Inter-AS traceback, there are several AS-level mechanisms that have been proposed [52]–[55].
- Real-time Inter-network Defense:
  There is need for Inter-AS communication which facilitates the traceback information exchanges between different autonomous systems. A standard RID (real-time inter-network defense) message format defined in RFC 6045 can be used so that the traceback information can be exchanged on a timely basis [56]. A set of incident coordination message necessary to communicate cybersecurity event, especially including traceback request and scenario, is described between relevant network entities.

3.8 Evaluation Criteria and Comparison of Traceback Mechanisms

This section describes the criteria for evaluating current traceback mechanisms in [7] as follows;

- Degree of ISP involvement:
  It refers to degree of ISP involvement when traceback is performed by trace administrator. Most traceback mechanisms assume that ISPs provide limited facility to enable traceback. A desirable traceback scheme would require low level of ISP involvement.
- Number of packets required for traceback:
  It refers to the number of packets which are used by an

Table 3 Comparisons of prominent IP traceback mechanisms.

Taxonomy		ISP involvement	No. of packets required	Memory requirement		Processing Overhead		Ability to handle DDoS attacks	Misuse by attacker	Knowledge of network topology
				Network	Victim	Network	Victim			
Traffic Monitoring	Controlled Flooding [17]	High	Large	None	None	High	None	Poor	Yes	Yes
	Input debugging [16]	High	Large	None	None	High	None	Poor	Yes	No
Packet Marking	PPM [22]	Low	Large	None	High	High	High	Good	Yes	No
	DPM [23]	Low	Large	None	High	High	High	Good	Yes	No
	AAM [24]	Low	Large	None	High	High	High	Good	No	Yes
Packet Messaging	iTrace [39]	Low	Large	Low	High	High	High	Poor	Yes	No
Packet Logging	Hash-based [42]	High	1	High	None	High	None	Good	No	No
Overlay network	CenterTrack [18]	High	1	Low	None	High	None	Good	Yes	No
Hybrid	Hybrid [48]	High	Large	Medium	Medium	High	Low	Good	Yes	No

attacker to identify the source of attack once the attack has been identified. A desirable traceback could trace the source address of attacker with a single packet.

- Memory requirement:
  It refers to amount of additional memory required on the network elements or a dedicated traceback server. Additional memory on the network element would be undesirable while additional memory on dedicated servers is tolerable. A desirable traceback mechanism would require limited amount of additional memory at the dedicated server and no additional memory at the network element.
- Processing overhead for traceback:
  It refers to amount of processing overhead at the intermediate network element or a potential victim host. A traceback scheme with minimal processing overhead of the intermediate network element or victim host would be preferred.
- Degree of bandwidth increase:
  It refers to additional amount of traffic required for traceback. The desirable traceback mechanism should have minimal or no increase of additional bandwidth.
- Ability to handles massive DDoS attacks:
  It refers to the ability of the traceback scheme to reflect how well the traceback scheme can identify the sources of DDoS attackers. The desirable traceback scheme should trace any attacks including DDoS attacks.
- Misuse by attacker:
  It refers to the ability of attacker to orchestrate an attack that will be untraceable. The possibility of misuse by attacker should be as low as possible for an ideal mechanism.
- Knowledge of network topology:
  Some traceback mechanisms require the knowledge of network topology to accomplish the traceback function.
- Robustness of traceback:
  It refers to capability of traceback mechanism to produce meaningful result even if some network elements involved in traceback have been subverted. The subversion happens due to errors from the mal-configuration of the network element or improper software patch.
- Effect of partial deployment:
  It refers to the degree of effectiveness of traceback when the traceback schemes are deployed partially within a single ISP. The effects vary from inability to producing meaningful traces.
- Scalability:
  It refers to the amount of additional configuration performed on the other network elements which are required to add a single network element. It indicates how the traceback scheme can easily be expanded. The scalability said to be good if only newly added network element requires configuration, while it is said to be poor if adding a single network element requires complete configuration of the rest of network elements require configuration. The desirable traceback mechanism should be scalable.
- Number of functions needed to implement traceback:
  It refers to the amount of additional functions which

are required to implement the given traceback scheme.
- Capability to trace transformed packets:
  It refers to the ability of the traceback scheme to identify the source of attackers even when the transformation of packets happens. The packet transformation is a packet modification when packet forwarding happens. The common transformations include Network Address Translation, where source and/or destination address of packet are changed, and duplication of packet for the multicast communication.

Table 3 shows the comparison of the prominent IP traceback mechanisms of each category in terms of some evaluation criteria which may be more critical than other criteria. Table 3 shows that each mechanism type has advantages and disadvantages over other mechanism type. To summary comparison results, the packet marking type requires high processing overhead to the network node, but low ISP involvement. The packet messaging type requires the high processing overhead to the victim node, but does not require knowledge of network topology. The packet logging requires no processing requirement to the victim node, but high ISP involvement. The overhead network type requires change of routing by the network. Therefore, an ISP administrator needs to select suitable traceback mechanisms taking into account its network capabilities and environments. From the deployment perspective, taking into account comparison result, the packet logging types may have some advantages for following reasons [4];

- It is difficult to deploy the overlay network type in an uncontrollable network, where the routing of the packets is inflexible.
- Deploying the packet marking type may have some difficulty in an ISP network that employs IPsec.
- It may be difficult to deploy the packet messaging type in the network with many firewalls as sometimes they ignore ICMP packets containing traceback information. Moreover, it may incur non-trivial extra traffic.
- Controlled Flooding type may work with the Internet, however, it floods excessive amount of unnecessary traffic over the network.
- Input debugging type may still be immature for implementation. Also, it has difficulties to trace non-traffic consuming attacks.

4. Application of Traceback Mechanisms to Protecting against DDoS Attack

This section describes a typical application of traceback mechanisms, that is, application to DDoS attacks [13]. DDoS attacks are characterized by large amounts of traffic from multiple sources destined for particular network end resources to render that resource unavailable to the intended users. Figure 4 shows a typical DDoS attack scenario. The target of the DDoS attack are the resources within domain/region 1, and the attack traffic comes from

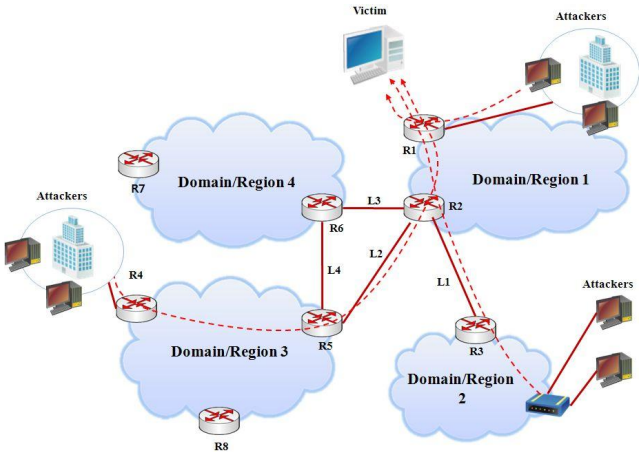

Fig. 4 Typical DDoS attack applications (Source: ITU-T X.tb-ucc [13]).

domain/region 1, and domains/regions 2 and 3 which belong to different network providers.

In DDoS attack, a victim wishes the network operator to block the attack traffic before it reaches them. It is difficult to identify the source of packets using traceback, however traceback is useful in identifying the ingress point and partial path of DDoS attack. This helps network operator use a traceback mechanism to determine the ingress edge router and affected high value links. In the DDoS scenario in Fig. 4, the quick solution is to block DDoS traffic at edge router R1. But if the attack traffic has reached R1, there has been a great deal of unwanted traffic flooding into the network, and this causes wasted network bandwidth. Therefore if traceback has been deployed in domains/regions 1, 2 and 3, and they cooperate in tracing network incidents back, routers through which DDoS traffic have been forwarded will be identified by use of traceback. Then there will be several better solutions, such as dropping the DDoS attack traffic by R4, the access device of domain/region2, and by R2, the ingress router of domain/region1, before the attack traffic reaches R1. If the DDoS attackers need to be located, the traceback is supposed to find the source of the DDoS packets based on sample packet, and be able to deal with spoofed packets.

5. Conclusion

The most practical way to prevent against the massive DDoS attack is to use a traceback technique to identify the attack source or attack path of this DDoS attack.

In this paper, plenty of different existing traceback mechanisms including global standardization activities that have been done by ITU-T SG 17 are surveyed. It addresses the taxonomy of the traceback mechanisms. In addition, the comparison of the existing prominent traceback mechanisms is presented in terms of several evaluation criteria such as the degree of ISP involvement, memory requirements, the number of packets required for traceback, knowledge of topology, capability to handle DDoS attacks, and

post mortem capability. The typical application example is also addressed.

References

[1] Massive DDoS attack returns to S.Korea, http:www.hani.co.krartienglish_editione_national466626.html
[2] White paper, "Analytical report on 3.4 DDoS attack," AhnLab, Inc., April 2011.
[3] H.Y. Youm, "Korea's experience of massive DDoS attacks from botnet," ITU-T SG 17, Tutorial presentation, April, 2011.
[4] T. Takahashi, H. Hazeyama, D. Miyamoto, and Y. Kodobayashi, "Taxonomical approach to the deployment of traceback mechanisms," Internet Communications (BCFIC Riga), Baltic Congress on Future, Februray, 2011.
[5] S. Vincent and J.I.J. Raja, "A survey of IP traceback mechanisms to overcome denial-of-service attacks," Recent Advances in Networking, VLSI and Signal Processing, University of Cambridge, UK, Feb. 2010.
[6] A. shahzad, R. Naseem, F. Adil, and S. Khayyam, "Trends in defensive techniques against denial of service (DoS) attacks," Canadian Journal on Network and Information Security, vol.1, no.1, pp.25–33, April 2010.
[7] A. John and T. Sivakumar, "DDoS: Survey of traceback methods," in International Journal of Recent Trends in Engineering, vol.1, no.2, pp.241–245, May 2009.
[8] L. Santhanam, A. Kumar, and D. Agrawal, "Taxonomy of IP traceback," Journal of Information Assurance and Security, pp.79–64, 2006.
[9] U. Kiran Tupakula and V. Varadharajan, "Analysis of traceback techniques," ACSW Frontiers '06 Proc. 2006 Australasian workshops on Grid computing and e-research - vol.54, 2006.
[10] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," SIGCOMM Comput. Commun. Rev., April 2004.
[11] A. Belenky and N. Ansari, "On IP traceback," IEEE Commun. Mag., pp.142–153, July 2003.
[12] H. Aljifri, "IP Traceback: A new denial-of-service deterrent?," IEEE Security & Privacy, vol.1, no.3, pp.24–31, 2003.
[13] H. Tian, H.Y. Youm, and T. Takahashi, "Revised text of X.tb-ucc: Usability of network traceback," ITU-T SG 17 TD 1592Rev.2, April 2011.
[14] H.Y. Youm, Y. Kadobayashi, H. Tian, and T. Rutkowski, "The 3rd revised text on draft recommendation ITU-T X.trm: Overview of Traceback Mechanisms," ITU-T SG17 TD 1780, April 2011.
[15] K.M. Moriarty and T. Rutkowski, "Revised draft recommendation ITU-T X.rid, Real-time inter-network defense," ITU-T SG 17, TD 1594 Rev.1, April 2011.
[16] T. Baba and S. Matsuda, "Tracing network attacks to their sources," IEEE Internet Comput. Mag., vol.6, no.3, pp.20–26, March/April 2002.
[17] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," USENIX, 2000.
[18] R. Stone, "CenterTrack," An IP overlay network for tracking DoS floods," USENIX, Aug. 2000.
[19] X. Wang, M. Brown, J.J. Yuill, C. Sargor, F. Jou, and F. Gong, "Deciduous: Decentralized source identification for network-based intrusions," Proc. 6th IFIP/IEEE Int'l. Symposium on Integrated Network Management, pp.701–714, 1999.
[20] D. Turk, "Configuring BGP to block denial-of-service attacks," Internet Engineering Task Force, RFC 3882, Sept. 2004.
[21] W. Kumari and D. McPherson, "Remote triggered black hole filtering with unicast reverse path forwarding (URPF)," RFC 5635, Aug. 2009.
[22] S. Savage, D. Wetherall, A. Kalin, and T. Anderson, "Network Support for IP Traceback," IEEE/ACM Trans. Networking, June 2001.
[23] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," IEEE Commun. Let., vol.7, no.4, pp.162–164, April 2003.
[24] D.X. Song and A. Perrig, "Advanced and authenticated marking scheme for IP traceback," IEEE INFOCOM, 2001.
[25] D. Dean, M. Franklin, and A. Stubblefield, "An algebraic approach to IP traceback," ACM Trans. Information and System Security, vol.5, no.2, pp.119–137, May 2002.
[26] V. Bhaskaran, A. Natarajan, and S. Sivanandam, "A new promising Ip traceback approach and its comparison with existing approaches," Information Technology Journal, vol.6, no.2, pp.182–188, 2007.
[27] T.W. Doeppner, P.N. Klein, and A. Koyfman, "Using router stamping to identify the source of IP packets," CCS, 2000.
[28] H. Alwis, R. Doss, P. Hewage, and M. Chowdhury, "Topology based packet marking for IP traceback," ATNAC, 2006.
[29] A. Yaar, A. Perrig, and D. Song, "FIT: Fast Internet traceback," INFOCOM, March 2005.
[30] M.T. Goodrich, "Probabilistic packet marking for large-scale IP traceback," IEEE/ACM Trans. Netw., vol.16, no.1, pp.15–24, 2008.
[31] M.T. Goodrich, "Efficient packet marking for large-scale IP traceback," CCS, 2002.
[32] L. Lu, M.C. Chan, and E.-C. Chang, "A general model of probabilistic packet marking for IP traceback," ASIACCS, 2008.
[33] A. Yaar, A. Perrig, and D. Song, "PI: A path identification mechanism to defend against DDoS attacks," Symposium on Security and Privacy, May 2003.
[34] A. Yaar, A. Perrig, and D. Song, "Stackpi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense," IEEE J. Sel. Areas Commun., Oct. 2006.
[35] A. Castelucio, A.T.A. Gomes, A. Ziviani, and R.M. Salles, "Intra-domain IP traceback using OSPF," LANOMS, 2009.
[36] M. Muthuprasanna and G. Manimaran, "Coloring the Internet: IP traceback," ICPADS, 2006.
[37] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic Packet marking: An IP traceback system to find the real source of attacks," IEEE Trans. Parallel Distrib. Syst., vol.20, no.4, pp.567–580, 2009.
[38] K. Choi and H. Dai, "A marking scheme using huffman codes for IP traceback," I-SPAN, May 2004.
[39] S. Bellovin, M. Leech, and T. Taylor, "ICMP traceback message," Feb. 2003, IETF, Internet Draft, draft-ietf-itrace-04.txt.
[40] A. Mankin, D. Massey, C.-L. Wu, S.F. Wu, and L. Zhang, "On design and evaluation of intention-driven' ICMP traceback," Proc. IEEE Int'l Conf. Computer Comm. and Networks, pp.159–165, 2001.
[41] B.-T. Wang and H. Schulzrinne, "A denial-of-service-resistant IP traceback approach," Proc. IEEE 9th International Symposium on Computers and Communication, (ISCC), vol.1, pp.351–356, June/July 2004.
[42] A.C. Snoeren, "Hash-based IP traceback," SIGCOMM, 2001.
[43] S.M. Bellovin and W.R. Cheswick, "Privacy-enhanced searches using encrypted bloom filters," 2004.
[44] A.C. Snoeren, C. Partridge, L.A. Sanchez, C.E. Jones, F. Tchakountio, B. Schwartz, S.T. Kent, and W.T. Strayer, "Single-packet IP traceback," IEEE/ACM Trans. Netw., vol.10, no.6, pp.721–734, Dec. 2002.
[45] M. Sung, J. Li, J. Xu, and L. Li, "Large-scale IP traceback in high-speed Internet: Practical techniques and information-theoretic foundation," IEEE/ACM Trans. Netw., vol.16, no.6, pp.1253–1266, Dec. 2008.
[46] W. Strayer, C.E. Jones, F. Tchakountio, and R.R. Hain, "SPIE-IPv6: Single IPv6 packet traceback," Nov. 2004.
[47] L. Zhang and Y. Guan, "Topo: A topology-aware single packet attack traceback scheme," Securecomm Workshops, Sept. 2006.
[48] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distrib. Syst., vol.19, no.10, pp.1310–1324, Oct. 2008.
[49] B. Al-Duwairi and M. Govindarasu, "Novel hybrid schemes em-

ploying packet marking and logging for IP traceback," IEEE Trans. Parallel Distrib. Syst., vol.17, no.5, pp.403–418, May 2006.
[50] S. Malliga and A. Tamilarasi, "A hybrid scheme using packet marking and logging for IP traceback," Int. J. Internet Protocol Technol., vol.5, no.1/2, pp.81–91, April 2010.
[51] T. Korkmaz, G. Chao, L. Trinh, and K. Sarac, "Single packet IP traceback in AS-level partial deployment scenario," Int. J. Securing Network, vol.2, no.1/2, pp.95–108, 2007.
[52] C. Gong, T. Korkmaz, K. Sarac, and S.G. Dykes, "Single packet IP traceback in AS-level partial deployment scenario," GLOBECOM, 2005.
[53] H. Hazeyama, Y. Kadobayashi, M. Oe, and R. Kaizaki, "Intertrack: A federation of IP traceback systems across borders of network operation domains," ACSAC, Technology Blitz Session, 2005.
[54] H. Hazeyama, Y. Kadobayashi, D. Miyamoto, and M. Oe, "An autonomous architecture for inter-domain traceback across the borders of network operation," ISCC, 2006.
[55] A. Castelucio, A. Ziviani, and R. Salles, "An AS-level overlay network for IP traceback," IEEE Netw., vol.23, no.1, pp.36–41, 2009.
[56] K. Moriarty, "Real-time Inter-network defense (RID)," Internet Engineering Task Force, RFC 6045, Nov. 2010.

Heung-Youl Youm received his PhD degree in Electronics Engineering from Hanyang University, Seoul, Korea in 1990. He received his Master and Bachelor degree in Electronics Engineering from Hanyang University, Seoul Korea, in 1981 and 1983, respectively. Currently, he is a Professor in the department of information security engineering at the Soonchunhyang University, Korea. He is the president of KIISC (Korea institute of information security and cryptology) in 2011. He has been a vice-chairman of ITU-T SG17 and a chairman of ITU-T WP 2/SG 17 since 2009. He had been working for the former MIC (Ministry of Information and Communication), Korea as a Project Manager for information security, from November 2006 to February 2008. His current interest includes theoretical and practical study on various security technologies/protocols such as IPTV/USN/NGN security. He had been an editor-in-chief for the KIISC Journal for KIISC (Korea Institute of Information Security and Cryptology) from January 2008 to December 2009, respectively. Since 2005, he has contributed to ITU-T by serving as an editor of five approved ITU-T Recommendations such as Recommendation X.1034 (Guideline on extensible authentication protocol based authentication and key management in a data communication network), X.1111, X.1131, X.1151 and X.1191 and several ITU-T draft Recommendations under development such as ITU-T X.iptvsc-3 (Key management for IPTV services), X.csi (Guideline on cybersecurity index), ITU-T X.tb-ucc (Usability of network traceback) and X.trm (Overview of traceback mechanisms).