Hindawi
Security and Communication Networks
Volume 2021, Article ID 6694650, 16 pages
https://doi.org/10.1155/2021/6694650

Research Article

Security-Oriented Network Architecture

Weiyu Jiang, Bingyang Liu, Chuang Wang, and Xue Yang

Huawei Technologies, Beijing, China

Correspondence should be addressed to Weiyu Jiang; jiangweiyu1@huawei.com

Received 16 October 2020; Revised 25 April 2021; Accepted 9 May 2021; Published 27 May 2021

Academic Editor: Salvatore D'Antonio

Internet benefits societies by constantly connecting devices and transmitting data across the world. However, due to the lack of architectural built-in security, the pervasive network attacks faced by the entire information technology are considered to be unending and inevitable. As Internet evolves, security issues are regularly fixed according to a patch-like strategy. Nevertheless, the patch-like strategy generally results in arms races and passive situations, leaving an endless lag in both existing and emerging attacking surface. In this paper, we present NAIS (Network Architecture with Intrinsic Security)—a network architecture towards trustworthiness and security. By solving stubborn security issues like IP spoofing, MITM (man-in-the-middle) attacks, and DDoS (distributed denial of service) attacks at architectural level, NAIS is envisioned to provide the most secure end-to-end communication in the network layer. This paper first presents a comprehensive analysis of network security at Internet range. Then, the system design of NAIS is elaborated with particular design philosophies and four security techniques. Such philosophies and techniques intertwine internally and contribute to a communication environment with authenticity, privacy, accountability, confidentiality, integrity, and availability. Finally, we evaluate the security functionalities on the packet forwarding performance, demonstrating that NAIS can efficiently provide security and trustworthiness in Internet end-to-end communication.

1. Introduction

The Internet protocol (IP) as the vital waist in the protocol stack forwards packets all over the world. However, endless security issues like IP spoofing, privacy breach, and denial of service attacks still threaten the current Internet. Due to the lack of security considerations in the original design of Internet infrastructure, patches to improve Internet security are hysteretic and inefficient in defending various network attacks. With massive heterogeneous devices accessing the network, the network environment becomes more complicated and security issues become more outstanding to hinder the widespread use of the emerging network techniques.

By analyzing the issues of existing IP protocols, there is a big challenge to balance authenticity, privacy, and accountability. IP address spoofing is attackers' customary tactics to avoid being filtered and tracked. There are still 1/3 autonomous systems permitting IP spoofing [1]. This destroys authenticity and provides convenience for distributed reflective denial of service (DRDoS) attacks [2]. Actually, a static and verifiable IP address is expected to prevent IP spoofing. However, mobility makes blacklist filters with static IP addresses less effective, and it is also difficult for the destination to identify spoofed packets when verification at the source fails. If the authenticity of IP addresses exposed in the header is guaranteed, accountability will be easily achieved to identify, track, and filter illegal traffic. However, it may bring big threats for senders' privacy. Privacy-curious entities can identify senders' identities and track locations based on authentic IP addresses. Attackers can infer other privacy information by correlating different activities based on nondynamic IP addresses.

It is widely accepted that the confidentiality and integrity of the packet payload can be protected by security protocols (e.g., IPsec and TLS). However, security of all these protocols is based on secure key exchange. Without efficient authentication, victims may be cheated to exchange a key with an attacker in the middle, which can hack the Diffie–Hellman key exchange process. Even though MITM attacks can be prevented by adopting the public key infrastructure (PKI) mechanism, the single point of failure or

unilateral misbehavior of the centralized authority becomes a new and worse problem. Moreover, heavy public key infrastructure (PKI) mechanisms may be infeasible for most resource constrained IoT devices to transfer and verify PKI certificates.

Additionally, the number of DDoS attacks, as one of the top threats that destroy network availability, reached 4.8 million in the first half of 2020 [3]. With attack amplitudes in the 2.3 terabit per second scale [4], not only the targets of the attacks were affected but collateral damage may take down many different remote sites. Although academia and industry have made efforts to offer defense mechanisms, DDoS issues cannot be fundamentally solved. Most proposals require high-cost hardware or software updates, and it is difficult to enforce the deployment of these proposals in Internet. With the addition of billions of heterogeneous, easy to compromise IoT devices to the Internet, the magnitude of the problem has grown even more [5]. The assumption that devices can be trusted inside a management domain is untenable, and a lot of attacks may happen inside the domain.

Motivated by solving these stubborn security issues, we carry out a detailed security analysis of end-to-end communication and have an insight into the root weaknesses of IP networks. Firstly, the IPv4 or IPv6 addresses with identity and location semantics lack the features of self-verification and privacy protection. Without dynamic, unforgeable yet privacy-preserving identifiers, it is hard to achieve authenticity, accountability, and privacy simultaneously. Secondly, the most pervasive forwarding devices like routers and switches only act as the dumb pipe to transfer IP packets without security functions to filter spoofed and malicious traffic. Expensive middle boxes like firewalls and intrusion detection systems cannot be deployed 1 : 1 with the forwarding devices; thus, all the traffic should be redirected to the security devices, which results in inefficiency and latency. Finally, there is a lack of efficient collaboration, especially cross-domain collaboration, among end devices and network forwarding devices to defend attacks like DDoS attacks, which cannot be solved by security solutions deployed in a single device or a single domain.

To eliminate the inherent security weaknesses of the existing IP networks, we present a network architecture with intrinsic security, called NAIS, which offers trustworthy security for end-to-end communication. There are four key techniques in NAIS: (a) minimum-trust-based authenticity verification to cure IP spoofing, (b) accountable and privacy-preserving dynamic identifiers based on ID and location separation, (c) decentralized and ID-built-in cryptographic key infrastructure which constructs the trust anchor to secure communication, and (d) collaboration-based inter-domain attack defense and tracing technique to mitigate malicious attacks.

More specifically, NAIS makes use of (1) ID and locator separation: decoupling identity (ID) and location (locator) from current IP addresses and using short-term ID and credentials to guarantee identity authenticity in control plane, dynamically encrypted ID in data plane to prevent illegal tracking, and partial encrypted locator to support routing and protect location privacy; (2) more flexible identifiers embedded in IP packet header to support user-defined security verification and cross-domain collaboration; and (3) ID-built-in cryptographic keys: host identifier is bound with the identity key to secure key exchange. Contributions of NAIS can be summarized as follows:

(i) We propose a new network architecture with trustworthiness and security characteristics, which provides a decentralized trust anchor without any single root of trust and eliminates the weaknesses of current IP networks.

(ii) We present a robust privacy protection scheme for IP packets in data plane, which can support packet-level privacy to prevent illegal tracking and correlation analysis.

(iii) Flexible IP header design towards minimal-trust model to support multistep fast verification and filtering. By embedding flexible identifiers, forwarding devices in the path can identify legal packets and filter illegal packets based on symmetric cryptography.

(iv) Extensive experimental results demonstrate that our security functions implemented in data plane have little effect on packet forwarding performance, and our scheme can support line-rate packet forwarding with hardware acceleration.

In this paper, we firstly analyze security issues and requirements of existing end-to-end communication in Section 2. Then, we give a system design of NAIS in Section 3 and illustrate the specific design of four security techniques in Section 4. The performance evaluation is given in Section 5. Finally, we summarize the conclusions and discuss future work in Section 6.

2. Security Issues and Requirements Analysis

As current IP addresses are coupled with multiple meanings, "identity," "address," and "accountable identifier," the inherent weakness that is too heavy burden on the unique IP identifier makes it hard to satisfy all the security requirements simultaneously. We give an overview map of security issues and requirement analysis of end-to-end communication process in Figure 1. The detailed analysis of authenticity, privacy vs. accountability, confidentiality and integrity, and availability is discussed in this section.

2.1. Authenticity and Accountability. IP spoofing within the source network is a persistent threat that damages authenticity. It is always adopted by attackers to launch session hijacking, MITM attacks, and DDoS attacks, and it is an essential ingredient of DRDoS attacks. Without an efficient verification of IP addresses, attackers can easily generate a spoofed IP address in the header, especially in the first packet, to cheat innocent nodes and make accountability infeasible.

In order to mitigate IP spoofing, many antispoofing approaches (IEF [6], uRPF [7], SPM [8], hop-count filtering

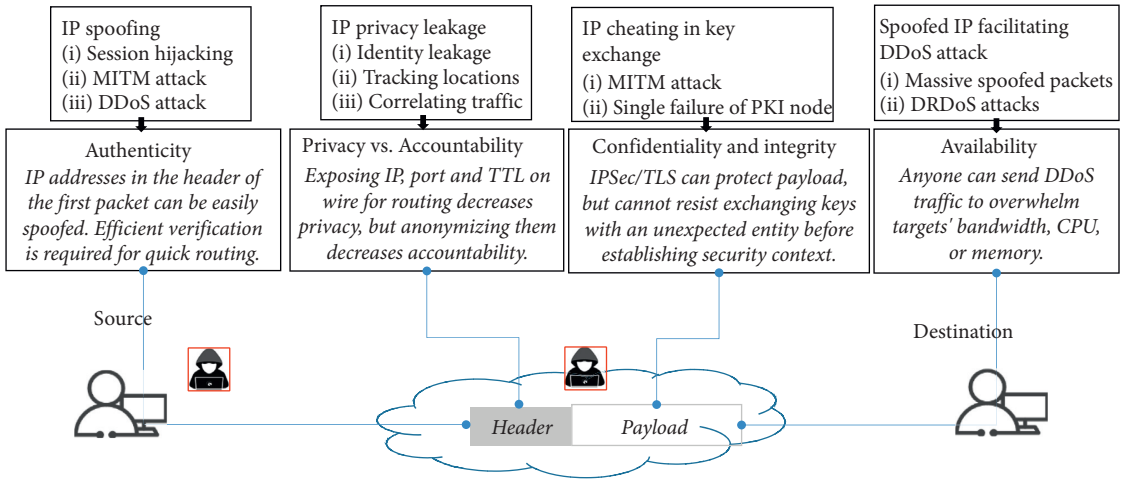


Figure 1: End-to-end security analysis.

[9]) have been proposed. The existing antispoofing solutions consist of three techniques: egress filtering in the source domain, ingress filtering in the destination domain, and cooperation-based interdomain filtering [10]. Both egress filtering and ingress filtering are implemented in routers or switches by configuring access control lists (ACLs). However, ACL proved to be complex and hard to manage. Moreover, most ingress filtering methods are too inflexible to cope with dynamic topology and always have low filtering accuracy since self-learning would incur false positives. Additionally, autonomous systems (ASes) lack incentive to deploy egress filtering mechanisms like SAVI [11]. Even if egress/ingress filtering solutions are deployed, it is still difficult for the victim host to identify the spoofed IP packets that have been carefully constructed, and these approaches may not work on traffic encrypted by IPsec or Tor. For example, uRPF which has been implemented in many routers cannot prevent attackers from the same subnet.

In fact, efficient defense techniques require ASes' cooperation to accurately identify spoofed IP addresses since single-fence model is inadequate to filter spoofed packets. SAVA [12] as an interdomain filtering mechanism prevents faked packets based on authentication tags sharing among autonomous system alliance. Path-based filtering [13, 14] is another interdomain technique, which verifies the packets by the path they flow through. However, most path-based filtering may bring a significant verification overhead for AS-level hop-by-hop processing.

Authenticity is the basis of providing accountability for a trustworthy network. In addition to IP addresses, more verifiable information is still needed to ensure packets' validity. However, in the existing IP networks, both network devices and end devices face challenges to identify illegal traffic just based on IP addresses. Even though existing solutions based on application layer data can filter some types of malicious traffic, they are time-consuming and are not fit for all the attack scenarios. For example, network devices cannot filter encrypted traffic between porn sites to children by checking domain name or application content. Besides, solutions deployed in the end devices can check the trustworthiness of sites to be visited based on the domain name, but users may still be misdirected to send IP packets to phishing websites without domain name resolution. Traffic from compromised public IP camera devices may still be forwarded to congest the victim game sites without checking by routers.

Therefore, authenticity and trustworthiness verification schemes need to be designed and deployed in the future IP networks. Network devices should have the ability to defend IP spoofing and distinguish illegal or unreasonable traffic based on IP layer data. With the entering of massive devices and with network environment becoming more complex, the assumption that only out-of-domain traffic is untrusted cannot keep a foothold. Attack traffic originated from the inner domain should also be considered Meanwhile, in order to maintain high speed of packet forwarding, verification with high performance is required to be implemented in multiple nodes against both uplink and downlink directions.

Compared with the existing solutions, our antispoofing technique in this paper is a multilevel authenticity verification including intradomain verification and interdomain verification. Neither complex and big ACL table is need, nor are sharing authentication tags used to identify spoofed packets. The authenticity verification functions implemented in routers are stateless and efficient based on fast symmetric cryptography. More identifiers with compound semantics including identity, attributes, and location are embedded in IP packet header, and all this information will be verified without breaking end-to-end security. Therefore, network devices can precisely determine whether a packet is spoofed or illegal.

2.2. Privacy vs. Accountability. It is contradictory to acquire both privacy and accountability in IP networks. The attention rate of privacy has risen in recent years, especially with the publishing of General Data Protection Regulation (GDPR). Users do not want their devices to be identified and traced by untrusted entities. IP-based correlation analysis makes boring ads more precise but brings deep privacy leakage risks to users.

Compared with other identifiers (cookies, browser fingerprints, device IDs, etc.), IP addresses embedded in the packets cannot be deleted or hided since they must be exposed for routing. However, IP addresses are adopted by most services to implement cross-browser tracking and even cross-device tracking. In the user side, we need an anonymous, untraced, and uncorrelated dynamic IP for privacy consideration. In the network side, an authentic, traceable, and permanent identifier is expected to support accountability for identifying, tracing, and shutting off illegal traffic. However, IP addresses which serve as both identity identifier and location identifier are unable to match paradoxical dynamic and permanent requirements from privacy and accountability.

Even though privacy and accountability have been researched for decades, there exist no perfect solutions to solve the contradictory issue.

Passport [15] and ISP privacy [16] can preserve privacy of source IP addresses but cannot hide the original ISP information. Mailbox [17] shared by multiple nodes to receive packets can hide authentic destination IP addresses, but it lacks source privacy. Onion networks (Tor [18–20]) are assumed to be efficient techniques that provide sufficient privacy, but these solutions are challenged by protocol incompatibilities and demanding cryptographic processing on constrained IoT devices [21]. Moreover, they have drawbacks with regard to achieving perfect privacy [22] and high performance. Although the privacy of IPv6 addresses has been paid attention by researchers, most works of IETF (temporary addresses [23], SLAAC [24], DHCPv6 [25]) only focus on the latter 64 bit interface identifier, instead of prefix privacy. In fact, the prefix in 5G which uniquely identifies the sender of IPv6-type PDU Session can also bring privacy issues. When the prefix is only shared by a small set of users, identity privacy as well as location privacy may also suffer from leakage threat.

In order to provide accountability, several approaches (AIP [26], APIP [27], APNA [28]) have also been provided by researchers. However, AIP only works for accountability and ignores privacy. APIP only considers source address privacy, and spoofed packets can also pass as not all packets are verified. APNA well achieves privacy and accountability by bringing in ephemeral ID but relies on frequent PKI certificates' requests and responses to resist correlation analysis of the same public key.

From the above analysis, it seems impossible to acquire both privacy and accountability due to the inherent flaw of IP addresses' multiple roles. In fact, identity identifier and location identifier can be detached from IP addresses. To support identity privacy and accountability, a verifiable privacy identifier is to be designed, so that real identity can only be checked and discovered by small legal authorities.

Compared with overlay privacy solutions like onion routing, our technique is inherently implemented in network layer by routers. The privacy of IoT traffic can also be protected in this paper. To support location privacy and routing, a partial encrypted locator with minimal privacy disclosure is implemented. By separating ID and locator, our method can achieve packet-level privacy. However, some existing methods in IETF cannot achieve this goal. In addition, the authentic identity is hided in the encrypted identifiers of IP header. Therefore, we can achieve fast accountability without step by step tracking and big table searching.

2.3. Confidentiality and Integrity. It is widely accepted that the confidentiality and integrity of sensitive data should be guaranteed by cryptographic techniques. In order to protect sensitive data in the payload of IP packets, TLS/SSL or other upper security protocols can be adopted, and we can also achieve confidentiality of data in the IP header by IPsec tunneling mode. However, security of all these protocols is based secure key exchange. If the process of key establishment is not trustworthy, data security may become empty words.

Dynamic key exchange is extensively adopted in the Internet, compared with static and inflexible preshared key approaches. Diffie–Hellman key exchange [29, 30] is a widely used method to dynamically exchange cryptographic keys over a public channel, but it suffers from man-in-the-middle attacks [31–33] without entity authentication. In order to resist MITM attacks, two different types of authentication methods are proposed: shared symmetric key-based methods and PKI certificate-based methods. However, symmetric key-based methods need out-of-band key distribution mechanism. The PKI certificate-based methods are flexible about authenticating entities without any preshared information. However, there are three types of weaknesses in the existing PKI, which can be adopted by attackers to launch MITM attacks in the TLS protocol. Firstly, the trust anchor CA may issue illegal certificates for single point failure of centralized PKI [34], and there is no boundary limit of CA certificates as any CA can issue any certificate for any entity. Secondly, it lacks efficient management of root certificates in the clients since an illegal root certificate may be easily implanted in the client by attackers. Thirdly, revoked certificate list may not be efficiently verified at the clients.

Therefore, there are still a lot of issues to be solved when exploring dynamic and secure key exchange solutions. To eradicate identity spoofing in end-to-end communication, constructing decentralized trust anchor may be a main trend.

2.4. Availability. DDoS attack is still a stubborn issue to be solved for providing availability in the network. The Mirai botnet, composed primarily of embedded and IoT devices, took the Internet by storm in late 2016 [35]. With more and more IoT devices connecting to the network, the situation may be aggravated in the future. As the goal of 5G, about 1 million device connections in only 1 square kilometers [36], will be supported by the network. Therefore, DoS attacks from the inner network also should not be underestimated.

In terms of mitigating the threat of DDoS attacks, academia has made efforts to offer promising defense mechanisms including rule-based methods [37, 38] and statistics-based methods. The rule-based methods can effectively filter

known attack traffic but cannot cope with complex unknown or encrypted attack traffic. Although unknown attack packets can be identified based on data mining [39], machine learning [40, 41], and AI [42], the accuracy mostly depends on the training dataset.

Due to lack of security consideration when designing the network at the beginning, anti-DDoS solutions in industry are mainly BGP blackhole [43, 44] and traffic scrubbing implemented in expensive and proprietary hardware appliances (deployed in-house or in the cloud [45, 46]). Regarding BGP blackhole, it discards malicious traffic and legitimate traffic indiscriminately, and the victim still cannot provide normal services. Traffic scrubbing is a postponed solution which brings delay by analyzing application layer data. Dots [47] can be assumed to be an inherent method to mitigate DDoS attacks. However, it lacks efficient incentive mechanism to motivate inter-AS cooperation. In addition, most approaches cannot detect and prevent DDoS in the edge of network or near the source; the service will soon be unavailable when DDoS traffic arrives at the victim. In a word, without resource advantages, it is still laborious for current patch-like defense approaches to resist overwhelming DDoS traffic.

Compared with the existing anti-DDoS solutions, our method is a collaboration-based multilevel anti-DDoS scheme. Firstly, we can prevent DDoS traffic with spoofed identifiers in the source domain. Secondly, we can also filter spoofed traffic from dishonest domains at the border router of the destination domain. Even if filtering at the border router fails, we still can identify most legal traffic by routers in front of the victim. Finally, we can also request the cooperated domains to filter malicious traffic near the source. All the filters are efficiently implemented in routers based on authenticated identifiers of network layer. However, routers in the existing network have no perfect methods to identify attack traffic without analyzing application layer data. Solutions which bring much overhead and redirection latency are always deployed in specific security devices like firewalls. Our methods which include anti-spoofing technique and user-defined identifiers in network layer can accurately and efficiently identify most DDoS packets by routers in the path.

3. NAIS Design Overview

This section describes the system design of NAIS. We firstly introduce five core network functions with security ability and then give the assumptions and the threat model. Finally, an end-to-end communication example is given.

3.1. Core Network Functions. We divide end-to-end communication into interdomain communication and intradomain communication. The trust anchor of interdomain communication is a decentralized ID and public key infrastructure to eliminate the threat of single point failure. Every autonomous domain has its own management policies and boundary. On the one hand, every domain defines its own policies to achieve source authenticity, accountability, and privacy. On the other hand, every domain provides ID and credential management for its nodes and provides proofs for the traffic originated in it to support interdomain authenticity verification and source tracing.

Figure 2 shows five core types of network functions in every domain: identity manager (IDM), accountability agent (AA), ID authenticator (IDA), ID router (IDR), and border router (BR). IDM is responsible for managing entity identity and issuing ephemeral anonymous certificates (including global anonymous identifier EID) to the host. AA is responsible for tracing illegal traffic. IDA authenticates the host and issue keys used in data plane to the host. IDR is used to provide authenticity for its outgoing packets, filter DDoS traffic, and also provide optional privacy service for hosts. Border routers are responsible for interdomain authenticity verification, and location privacy is also enforced by border routers. In NAIS, routers in data plane adopt symmetric cryptography techniques to provide packet-level authenticity and privacy. The definition of all the symbols used in this paper is given in Table 1.

We present four key techniques in the following:

(i) Minimum-trust-based authenticity verification. There is no complete trust in interdomain traffic or intradomain traffic. The authenticity of traffic of both uplink and downlink can be guaranteed. When a packet is transmitted, it is verified by both the routers in the source domain and the routers in the destination domain.

(ii) Accountable and privacy-preserving dynamic ID/locator. Dynamic ID and locator which confuse unauthorized entities are used to prevent privacy breach and correlation analysis. The entity outside the source domain can only uncover a packet's domain information, rather than the specific location and senders' identity. When attacks happen, the victim can trace illegal traffic back to the source domain, and only the source domain can track the sender by opening the authentic ID and locator.

(iii) Decentralized and ID-built-in cryptographic keys. A decentralized key management scheme is applied to avoid single point failure. Key management is isolated by domains, which means that the compromise of domain key can only impact one domain, whereas a compromised authority in PKI can issue or revoke certificates without specific boundary. The identity keys to negotiate session keys are built-in in the host identifiers, and man-in-the-middle attacks can be completely eradicated.

(iv) Interdomain attack defense and tracing. Most spoofed traffic can be filtered by the intradomain routers and border routers in the destination domain. When DDoS attacks of large volume happen, the sender can embed an authentication identifier in IP header to get priority to pass verification in the destination. The victim host can also initiate a cross-domain attack defense protocol and request the source domain to filter illegal flow.

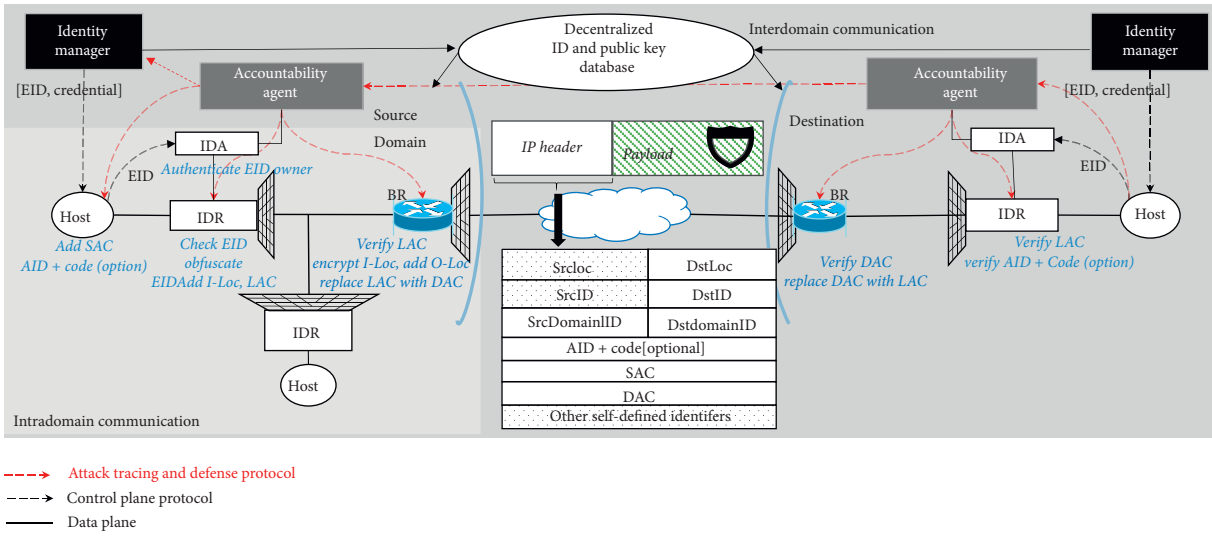


Figure 2: Network architecture with intrinsic security for end-to-end communication.

Table 1: List of used notation.

Notation	Description
IDM	Identity manager for managing identity and credentials
AA	Accountability agent for tracking the source identity
IDA	ID authenticator for authenticating an entity
IDR	ID router for verifying host ID authenticity
BR	Border router
HID	Host identifier
I-Loc	Inner locator for routing in the intradomain
O-Loc	Outer locator for routing in the interdomain
EID	Ephemeral and encrypted ID to identify a host
EI-Loc	Encrypted inner locator
EHID	Encrypted host ID
Code	Message authentication code
SAC	Source authentication code for host ID authenticity
DAC	Domain authentication code for domain ID authenticity
LAC	Location authentication code for locator authenticity
AID + Code	Authenticated user identifier and message authentication code
SrcLoc	Source host locator
DstLoc	Destination host locator
SrcDomainID	Source domain identifier
DstDomainID	Destination domain identifier
HK	A symmetric key owned by the host
MACKey	A symmetric key to protect layer-2 data
MK	A symmetric master key owned by border routers
VK and DK	A shared symmetric key to verify authenticity
SK	A symmetric key to encrypt data in IP header
PF	A privacy flag
DF	A dynamic factor which may be randomly generated

3.2. Assumptions and Threat Model. We assume that IDA in the control plane is honest to authenticate hosts but is curious to obtain or leak hosts' permanent and authentic identity. For instance, when a host from the trusted domain A moves to access domain B's network, the IDA in domain B firstly authenticates the host and try to obtain the authentic identifier of the host.

We also assume that legal border routers are honest to support authenticity verification and privacy protection for outgoing packets. This means that they sign the packets with secure cryptographic primitives to help the destination to verify the source authenticity. Besides, they also encrypt the specific inner locator in outgoing packets based on hosts' privacy policy. We do not assume that IDR at the edge in the source is secure enough to check authenticity. Both the host and IDR may try to forge the packets' origin. For instance, a host may use a spoofed ID in its sending packets, and a compromised IDR located in edge network may transfer

spoofed IP packets and may tamper the source identifier to avoid being traced.

For privacy consideration, the destinations and the entities on the links (host to IDR, IDR to BR, BR to destination) are curious to analyze the sender's specific locations and correlate activities of the same host. For example, a website may correlate the host current activity with the same host's other activities in other cooperated sites or in previous visits.

All the cryptographic primitives used in NAIS are assumed to be secure.

3.3. Communication Example. We describe the high-level workflow for communication between two hosts in Figure 2. The detailed workflow is described in Section 4. When the source host connects to the network, it firstly authenticates itself to the IDA in the access network. After successful authentication, the host establishes secure channel with IDR based on symmetric keys, and the access network acts as the source domain to provide secure packet forwarding service.

Network Access Procedure. The host firstly presents an ephemeral anonymous certificate to the IDA to authenticate itself. The ephemeral certificate issued by the IDM includes an encrypted ID (EID), public key, expire time, signature, and other information. The IDM may or may not belong to the same domain with IDA. Only the entities authorized by IDM can decrypt the encrypted ID to obtain the authentic and permanent identity. After a successful authentication, the IDA issues several symmetric keys to the host and the IDR. These keys are used in the data plane. The host and the IDR establish a security connection based on the shared symmetric key issued by the IDA.

End-to-End Communication Procedure. Before sending a packet, the source host generates and adds a source authentication code in the packet header. When the IDR in the source domain receives the packet, it firstly checks and obfuscates the source ID in the packet header. Then, it adds an inner locator and a location authentication code in the header to prove that the packet really comes from the claimed location. After the border router in the source domain receives the packet, it firstly verifies the source authentication code and the location authentication code. Then, it encrypts the inner locator and adds a domain authenticity code in the header to prove that the packet really comes from this domain. Finally, it transfers the packet. When the packet arrives at the destination domain, the domain authenticity code is firstly verified by the border router. The packet may also be verified by the IDR near the destination when the destination host suffers from DDoS attacks. After passing all the verification, the packet arrives at the destination host.

4. NAIS Detailed Design

NAIS aims at providing authenticity, accountability, and privacy for IP header information; confidentiality and integrity for the payload; and availability. All these security features are achieved by the four key techniques: (1) minimum-trust-based authenticity verification; (2) accountable and privacy-preserving dynamic ID/Loc; (3) decentralized and ID-built-in cryptographic keys; (4) interdomain attack defense and tracing. The detailed description of NAIS will be illustrated in the following subsections.

4.1. Minimum-Trust-Based Authenticity Verification. Minimum-trust-based verification is designed to block spoofed traffic from dishonest entities from both intradomain and interdomain. NAIS combines self-filtering of the source domain and interdomain verification to guarantee the authenticity of packets' origin.

We design distributed IDA to authenticate hosts in the control plane. With massive IoT devices connecting to the network, adopting distributed IDA improves the efficiency of authentication. Compared with the authentication protocol between a host and a remote centralized server, distributed authentication reduces the delay of authentication requests and responses. It also mitigates the DDoS attacks against a centralized authentication server and solves performance bottleneck issues of the centralized server. A host accesses the network by using a PKI certificate issued by any IDM, whose public key and user identifier space are recorded in the decentralized ID and public key database. The anonymous EID should match the user identifier space of the IDM. The IDA decides whether it accepts the certificate issued by this IDM based on its security policy or cooperation agreement with the IDM. The authentication protocol can be the EAP protocol [48] or other secure authentication protocols.

However, the existing authentication protocol for accessing the network like 802.1X [49] is not based on IP protocol since the host has not been issued an IP address before finishing authentication. An application proxy to transform authentication packets is implemented in the access point, and the existing authentication protocol has a very complex procedure which requires 3 or more RTTs. In our design, the authentication protocol for connecting to the network is simplified without an application proxy to conduct protocol translation. A unique ID in the network layer is used in the first authentication request packet for routing. Aiming at reducing overhead for authentication, the new authentication protocol can also be adopted by most constrained IoT devices.

The ID routers near the hosts are designed to take over the first step authenticity check in data plane. After successful authentication, several keys including HK and MACKey are issued to the host by the IDA. The HK is used to generate source authentication code and is only disclosed to the source host and the border router. The MACKey is used to establish a security connection on the link layer between the host and the ID router. The ID router shares a lot of symmetric keys with the other ID routers and the border routers in the same domain. To support the source authenticity, the border router uses a master key to verify source ID, and it uses symmetric keys shared with the ID

routers in the same domain to verify source locator. It also maintains a lot of symmetric keys shared with the border router in the other domains to support cross-domain verification. The detailed procedure of authenticity verification is shown in Figure 3.

For outgoing traffic, the host firstly uses HK (a symmetric key) to compute a SAC (source authentication code). The SAC in the packet header is used to prove that the packet is really generated by HID (source host ID) of the claimed host. When the packet arrives at the ID router, the ID router checks HID and adds I-Loc (an inner locator) and LAC (location authentication code) in the header. The LAC computed with VK (a symmetric key) is used to prove that the packet really comes from I-Loc claimed region. VK is shared between the ID router and the border router. The border router then verifies LAC, and it performs sampling verification on SAC. The HK to verify SAC is derived from HID and MK (a master key), so that no per host status is maintained by the border router. By randomly verifying SAC, the border router decides whether the IDR is compromised. Therefore, packets with spoofed EID or spoofed locator will not be forwarded by routers. After successful verification, the border router generates DAC (a new domain authentication code) to replace the LAC. The DAC is also a message authentication code calculated with DK (a symmetric key), which is shared with the destination domain.

For incoming traffic from outside domains, the border router in the destination domain verifies the authenticity and forwards packets to the correct host. Firstly, the border router queries its database to obtain the symmetric key DK based on the source domain ID. Then it verifies the DAC with DK. If the packet passes verification, the border router replaces the DAC with a new LAC. LAC is calculated with the key VK shared between the BR and the ID router near the receiver. The LAC in this step is used to prevent an inner dishonest host via a compromised ID router from forging outer domain packets. Finally, the packet is forwarded by the BR to the IDR.

For incoming traffic from ID routers inside the domain, the ID router near the destination host verifies the LAC to filter spoofed traffic. For example, in the mobile edge computing scenario, every two ID routers share a symmetric key. For intradomain communication, the IDR near the sender generates LAC with a VK. The VK shared with the IDR near the receiver is used to verify LAC and prevent spoofed packets from intradomain. Only packets with correct LAC can be transferred by the destination IDR.

By separating hosts' identifier and network locator, we provide the authenticity of host identity and location. NAIS is scalable to support more self-defined identifiers in IP header. According to the requirement, both source hosts and network devices are able to embed unforgettable identifiers like security attributes to support fine-grained filtering. A packet with source identifiers can be filtered by multistep verification. Besides self-filtering in the source domain, we also make the destination domains have the ability to prevent spoofed packets. The dishonest behavior of hosts and network devices can be discovered via verification, and the goal to implement minimum-trust principle is achieved.

4.2. Accountable and Privacy-Preserving ID/Loc. NAIS well balances accountability and privacy by separating identity and location identifiers from IP addresses. Global ID as the host's ID and Loc (locator) as the least addressable region locator are embedded in the header of every packet. Efficient accountability is supported by adopting a global unique host identifier (EID) in IP header. It means that authorities can quickly identify the sender based on host ID without step by step tracing. Privacy is also achieved by using encrypted ID and locator. The activities in different websites or in different time slots of the same host cannot be correlated by privacy-curious websites and illegal eavesdropper. No entities outside the source domain can discover the specific location of the sender. The detailed procedure to generate and translate privacy ID and locator is shown in Figure 4.

Host identity privacy is achieved by obfuscating source identifiers in the ID router. The privacy on the link from the host to IDR is protected by a secure connection. Before initiating a new flow, the source host generates a new HID as the source ID in the header. The HID is composed of a privacy flag (PF), EID, and a dynamic factor (DF). For outgoing packets, based on the indication of PF, the IDR obfuscates HID (the source ID) with a secure encryption algorithm. By encrypting HID with IDR's private key (SK1), we can achieve different ciphertexts of the same host ID by inputting DF to resist privacy correlation analysis. For intradomain traffic, the destination host uses I-Loc (IDR's locator) and EHID (encrypted host ID) to uniquely identify the source host. For outgoing packets arriving at the border router, the BR generates EI-Loc by obfuscating I-Loc with its private key (SK2) and EHID. The destination host uses BR's locator (O-Loc), EI-Loc, and EHID to uniquely identify a source host. Our stateless obfuscation method can achieve "per flow, per source ID, per source locator" to resist cross-destination and cross-time correlation.

Location privacy is preserved by obfuscating source locator in the border router. When the packet with an inner locator arrives at the border router, the border router adds O-Loc (BR's locator) and encrypts the inner locator. Since the border router obfuscates I-Loc by inputting dynamic EHID, we can achieve different ciphertexts of the same inner locator with different EHID. Therefore, both address independence and locator privacy can be achieved. The obfuscation method brings two benefits: (1) only the outer locator which refers to the border router is exposed, and the inner locator is encrypted; (2) no entities outside the domain can infer whether two hosts are from the same location.

Every return packet correctly arrives at the receiver with stateless translating. Firstly, the return packets are forwarded to the border router based on the indication of outer locator (O-Loc). The border router retrieves encrypted locator information from the packet header and recovers the inner locator (I-Loc) by decrypting EI-Loc with its private key SK2. Then, the packet is forwarded to the IDR based on the plaintext of the inner locator. The plaintext of HID is recovered by the IDR with the reversible translating algorithm and SK1. Finally, the return packet is forwarded to the correct host based on HID.

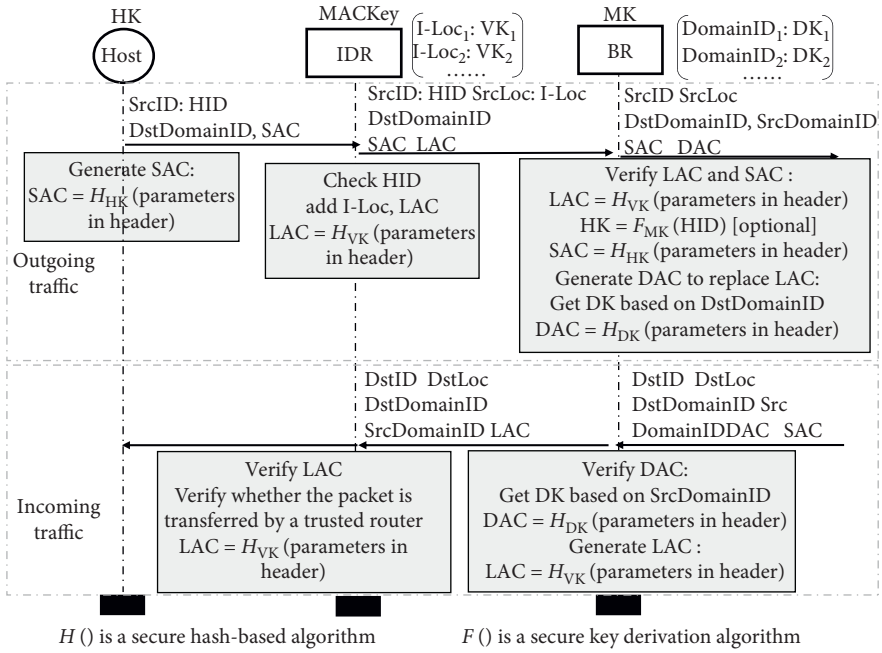
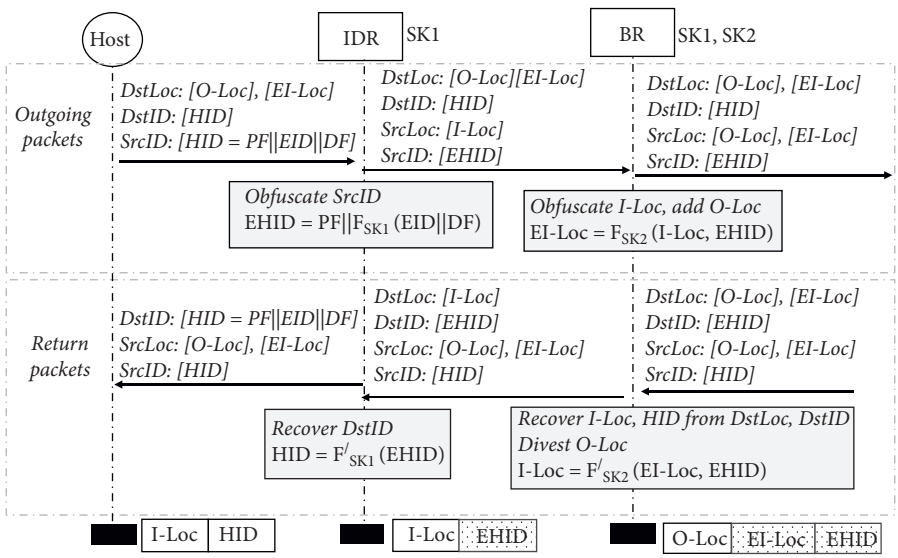


Figure 3: Authenticity verification procedure.



$F_{SK}()$ refers to an obfuscation algorithm with the secret key SK as the input
$F_{SK}/()$ refers to a de-obfuscation algorithm with the secret key SK as the input

Figure 4: The procedure to generate and translate privacy ID and locator.

By dynamically encrypting identifiers by routers, both privacy and accountability can be achieved. Compared with existing anonymous routing solutions, we can achieve packet-level privacy to resist correlation analysis in network layer. The privacy function inherent in routers can also benefit constrained IoT devices. Compared with the existing step by step tracking solutions, we determine the identity based on the global host ID instead of a local interface ID in IPv6 addresses. Using dynamic encrypted ID in NAIS only increases one decryption operation, and the overhead is negligible for an accountability agent (AA). When the sender of a packet is required to be tracked, AA can directly obtain the identity and location of the source host by decrypting the encrypted identifiers. Only when EID is used as the raw host ID, the AA needs to request the IDM to open senders' identity.

4.3. Decentralized and ID-Built-In Cryptographic Keys. The trust anchor of NAIS is a two-level decentralized public key database based on blockchain techniques. NAIS uses

global decentralized database to manage ID and public keys of public services and autonomous domains. The public key related to a public service or an autonomous domain cannot be modified and deleted by any single authority. For private services which can be accessed by only limited endpoints or local entities, local decentralized public key database is adopted to prevent single point failure. There are three advantages brought by decentralized public key databases: (1) risks from single point failure of CA are eliminated; (2) certificate verification chain is shortened from regular 3 or 4 certificates' verification to 1 or 2 certificates' verification; (3) the action scope of every root public key is limited and can be verified by entities.

Authenticated key exchange based on decentralized public key database is a required option in NAIS to prevent MITM attacks and other identity spoofing attacks. As is shown in Figure 5, before transferring sensitive data, two peers will conduct authenticated key exchange protocol to prevent MIMT attacks. In the scenario where client communicates with a public service's server, the client verifies the server's certificate which is signed by the public key recorded in the database. We assume that the client can securely retrieve the service's public key from the global database before it sends packets. During the certificate verification procedure, neither CA certificate nor root certificate is used in this case. In the scenario where a client communicates with private services' servers or endpoints inside the same domain, a root certificate which is signed by the domain public key will be used to verify the peer's certificate. Therefore, the length of certificate verification chain is no more than 2 in NAIS, and the weakness brought by middle CA can be eliminated.

The security of root certificate management is enhanced by designing certificate guard devices in every domain. In existing mechanisms, root certificate can be easily implanted in the client. Most endpoint devices may lack the ability to determine whether a root certificate should be trusted. If an illegal root certificate generated by an attacker is accepted by the client, then MITM attacks can be successfully launched. We use certificate guard to help the clients to securely manage root certificates. Every root certificate is verified by the certificate guard before the client accepts a root certificate. A root certificate for private or local use is signed by a domain public key, and it must be registered in the local database to support accountability. By binding the root certificate with a domain, the action scope of the root certificate is limited. It can only provide legality proof for the endpoints' certificates in the same domain. Another functionality of certificate guard is to help clients to conduct complete certificate revocation checking. In the existing solutions, most certificate revocation information cannot be directly retrieved by clients, and it brings much communication overhead for clients [50, 51]. To lighten clients' burden for obtaining and checking certificate revocation information, the certificate guard is designed to retrieve and cache fresh certificate revocation information. Since the certificate revocation information requested by clients from the same domain or organization is always similar, adopting certificate guards can improve efficiency and security for certificate revocation checking.

One of the main features in key exchange procedure is that the exchanged certificate binds host's network layer identifier (e.g., ID in IP layer) with a public key. In the existing solutions, PKI certificate binds web service's domain name with a public key to resist MITM attacks. In the scenario where a service provider uses many edge servers or CDN servers to provide services, the service certificate and private key are always shared by all the servers to support the clients' verification. Obviously, compromising any edge server will bring security risks of key exchange. In NAIS, every endpoint has its own certificate which binds a network layer identifier. Therefore, compromising the private key of one edge server will not bring MITM attack risks to other servers' communication.

4.4. Interdomain Attack Prevention and Tracing. Filtering DDoS traffic in the domain border or near the attack source is one of our main goals by deploying cross-domain cooperation solutions. To reach the goal, we design three-level defense mechanism to prevent DDoS traffic. DDoS traffic is firstly prevented at the border router of the destination domain. Most spoofed traffic is filtered by the first defense. Then, attack traffic which passes through the first defense is filtered at the IDR near the victim. Only traffic with authentic identifiers can arrive at the victim, and abnormal big traffic can be identified and traced based on the authentic identifiers. The last defense is that the victim can use an attack defense and tracing protocol to request the source domains to clean the abnormal traffic.

The detailed description of the three-level defense against DDoS attacks is given as follows (Figure 6):

(i) The first defense at the border router. Packets with spoofed domain identifiers from dishonest domains can be prevented at the border routers of the destination domain. This is implemented by embedding the domain ID and a domain authentication code (DAC) in every packet. Every two domains share a symmetric key to generate DAC. Without a shared key between the source domain and destination domain, the packets with spoofed ID cannot pass through verification. If most attack traffic is confirmed to be from some specific domain and is not honestly blocked by the source domain, the destination domain can limit the traffic from the source domain according to its security policy.

(ii) The second defense at the ID router. NAIS shifts down the user identifier AID from the application layer into the network layer. AID is a verifiable ID which is distributed by the protected service. Registered user's hosts and service hosts inside the protection region are previously allocated with AID and related keys. There are two types of traffic marked with AID and code in the IP header. Every packet from the registered users is embedded with AID and a code which is computed by the key and dynamic parameters. Legal response traffic from reflective servers (e.g., DNS, NTP) is also marked

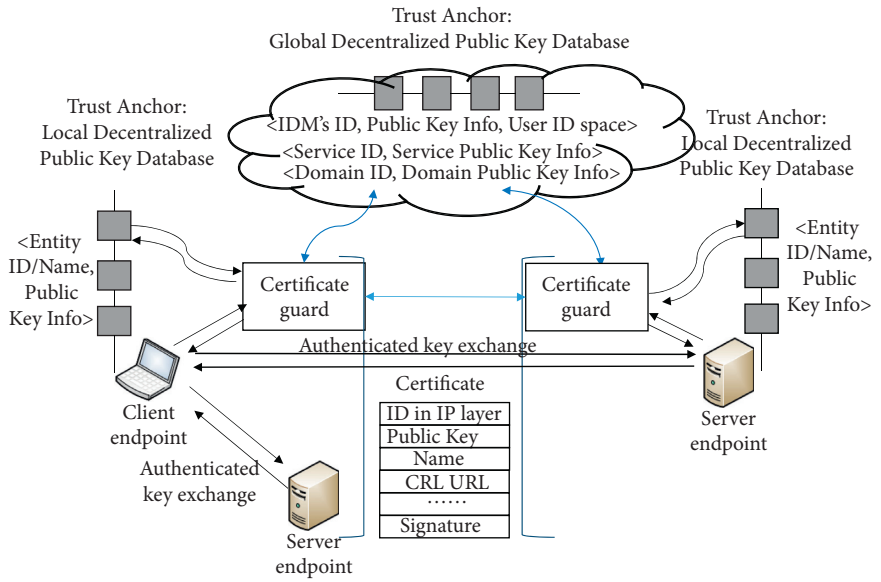


Figure 5: Decentralized public key database-based authenticated key exchange.

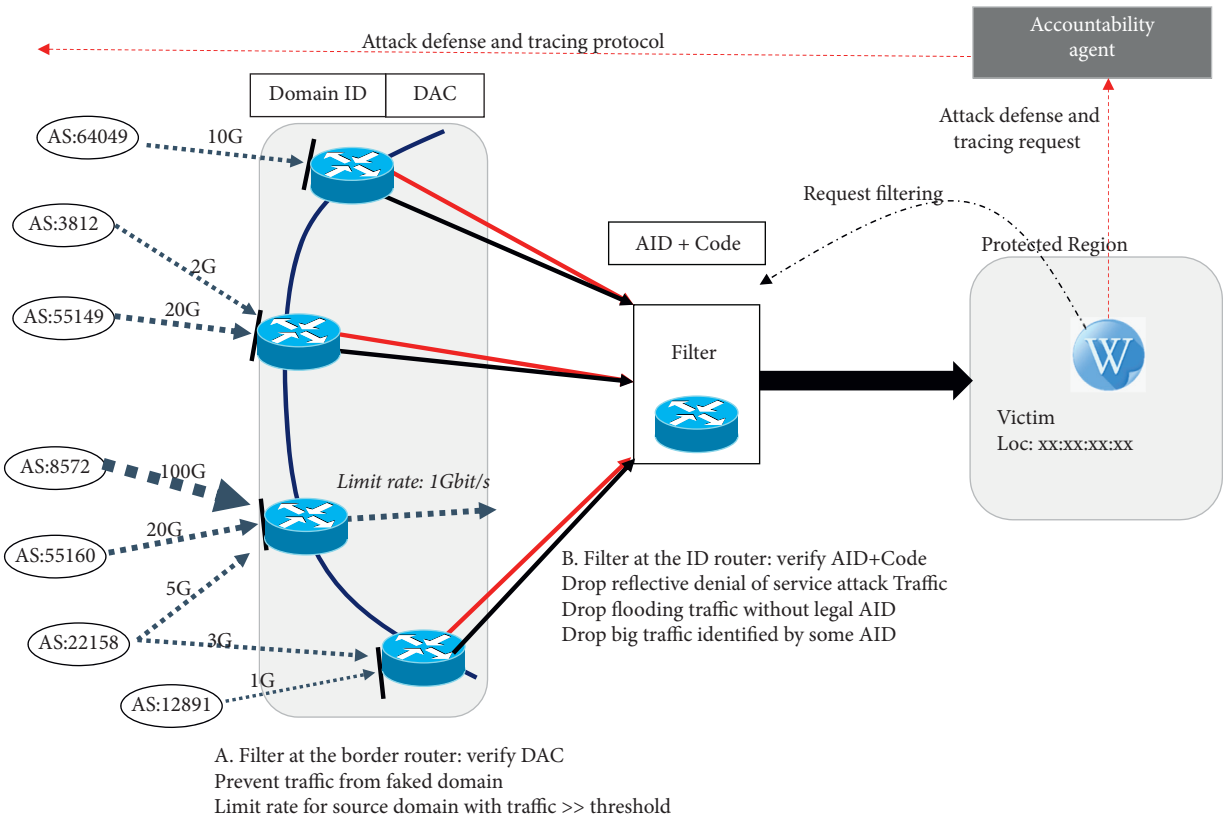


Figure 6: Interdomain DDoS attacks prevention.

with AID and code. By adopting AID and code in the network layer, network devices in front of the victim can efficiently filter illegal traffic. Therefore, reflective denial of service attack traffic and most flooding traffic can be efficiently dropped by network devices before arriving at the victim. The abnormal big traffic marked with the same AID can also be identified and dropped in this step.

(iii) The last defense at the victim host. An attack defense and tracing protocol is adopted to trace illegal traffic and prevent attacks near source. On the basis of the two previous filtering steps, most abnormal traffic

with authentic identifiers can be well determined at the victim. If the traffic is deemed to be abnormal, the victim initiates the attack defense and tracing protocol to push back the abnormal traffic to the source domain. Firstly, the victim sends a request with the illegal packet to the accountability agent in the destination domain. Then, the accountability agent propagates the request to the accountability agent in the source domain. Since privacy identifiers are adopted, only the source domain has the ability to trace the attacker's identity and location. When receiving the request, the accountability agent in the source domain firstly conducts nonrepudiation checking by verifying source authentication code (SAC) in the packet header. Then, it opens the authentic host identifier and location. Finally, it sends control commands to the related routers to take actions.

5. Implementation and Evaluation

We implement source authenticity verification, identifiers' privacy protection, and interdomain DDoS defense over IPv6. Although NAIS includes authentication protocols in control plane and decentralized key management functions, existing related solutions have proved that these techniques are feasible to implement. However, most packet forwarding devices like routers have no inherent cryptographic calculation functions, since they have high performance requirements for forwarding packets. Therefore, we focus on evaluating the performance of routers in data plane which performs cryptographic operations on every packet.

We use OMNeT++ INET as the simulation platform to carry out experiments to show the performance of packet forwarding. Since the cipher operations in the routers are similar, we only present performance evaluation of the ID router and the border router in this section.

5.1. NAIS Data Packet. As is shown in Figure 7, we embed network locators and host identifiers in IPv6 addresses with 128 bit length. A next header of IPv6 packets is adopted to add additional fields to support NAIS security functions. The dynamic factor (DF), domain identifiers, timestamp, SAC, DAC, and AID are located in the next header. The SAC, DAC, and AID code are the output of secure message authentication code (MAC) generation algorithms, with the input of SrcIP, DstIP, DF, SrcDomainID, DstDomainID, and TimeStamp. We take DF as the input of encryption algorithm to provide identifiers' privacy, and take timestamp as the input in the code generation procedure to resist replay attacks. Even though we give a length value of all the security fields, the length of these fields can be redefined according to specific requirements. We adopt AES-256 as symmetric cryptography to implement authenticity verification and identifiers' privacy. AES-CMAC which is secure for fixed length inputs is adopted to generate MAC. Host identifiers and inner locators are encrypted by using AES-256. In the future, we will implement lightweight symmetric cryptographic algorithms to achieve high performance.

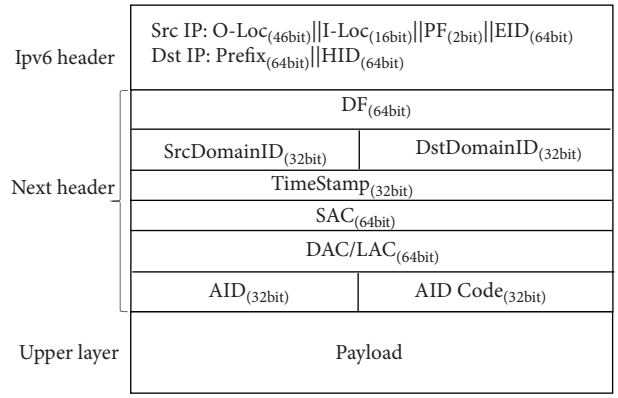


Figure 7: NAIS packet header.

5.2. ID Router Implementation and Forwarding Performance Evaluation. Compared with the regular router, the ID router near the source host additionally performs one encryption to obfuscate source ID and one MAC computation to generate LAC. The ID router near the destination host performs one MAC to verify AID code, and it may perform a key derivation calculation to get AID key based on a master key. If the related key of every AID can be obtained by searching a small key table, then the overhead for verifying AID code is just one MAC computation. Therefore, we only give the forwarding performance evaluation of the source IDR in Figures 8 and 9, since the IDR near the receiver performs fewer operations.

We perform a throughput evaluation experiment for 4 different packet sizes. We compare the performance of 4 types of ID routers: (1) the IDR without any security functions; (2) the IDR with authenticity verification function; (3) the IDR with ID obfuscation function; (4) the IDR with both verification and obfuscation functions. Since the source host's packet rate is limited on the simulation platform, we set a total capacity of 4 Gbps for the IDR.

As is shown in Figure 8, the IDR has adequate capacity to perform security processing without degrading performance for the given packet rates. Compared with the regular packet processing without adding security processing (shown by the noncurve), the throughput of the router which performs ID authenticity verification only drops by 0.18 Mpps or 23 Mbps. We also can infer that increasing encryption almost has no throughput drop. Figure 9 also shows that the delay increased by the cipher calculation on every packet header is no more than 100 ns. Therefore, the security operations are lightweight and will not degrade routers' performance.

In fact, the slight throughput drop and delay are brought by message authentication code calculation. In order to generate the message code (LAC), we take the information (IP addresses, DF, domain ID, TimeStamp) of 52 bytes as the input. Therefore, the CMAC algorithm needs to call AES about 6 times. If the implementation platform has parallel computing and hardware acceleration on cryptographic operations, the performance of packet forwarding will be largely improved. Another method to improve the performance can be adopting more lightweight cryptographic

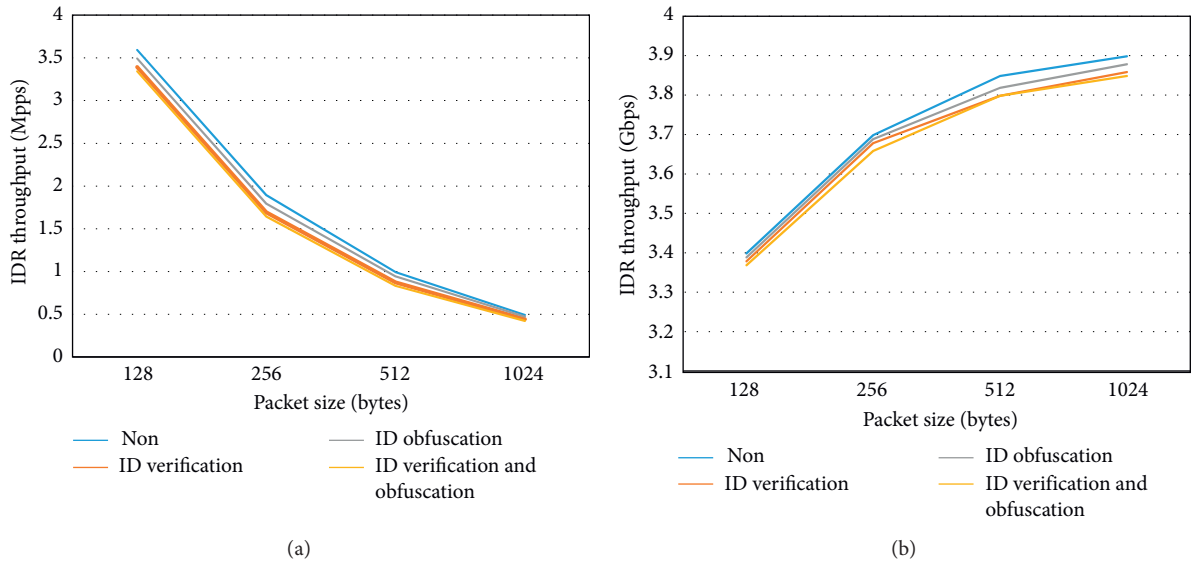


Figure 8: Forwarding performance of the ID router expressed as (a) packet rate and (b) bit rate.

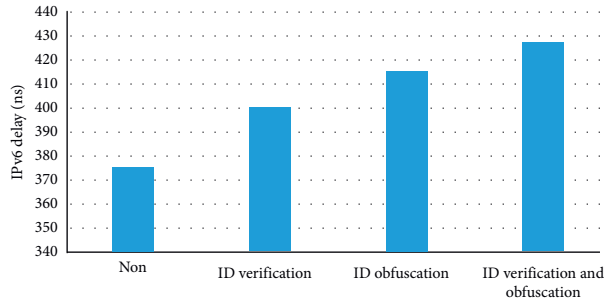


Figure 9: Packet delay on the ID router.

algorithms. In fact, reducing the length of input data which can be supported in our flexible IP header can also improve the routers' forwarding performance, since the IPv6 address is of fixed 16 byte length and more input data means more AES calling.

5.3. Border Router Implementation and Forwarding Performance Evaluation. The border router in the source domain basically performs two MAC calculations to verify LAC and generate DAC and one encryption to provide locator privacy. To prevent spoofed packets from compromising ID routers, the border router randomly performs one decryption to get host ID, one key derivation and one MAC to verify SAC. SAC generated by the source host is verified every 100 packets to check whether the IDR is secure and honest. When verifying SAC generated by the host, the border additionally performs one key derivation and one MAC computation. The key derivation algorithm is one of the HKDFs (hashed key derivation functions) based on HMAC-SHA256.

We set a total capacity of 10 Gbps for the border router to process traffic from three ID routers (4 Gbps from IDR1, 4 Gbps from IDR2, and 2 Gbps from IDR3). Figure 10 shows that the additional security operations have minor impact on the performance of the border router. Compared with the performance of the BR with no security functions shown by noncurve, the ID verification operations only bring 0.3 Mpps or 38 Mbps drop of the throughput shown by the ID verification curve. As shown by the ID obfuscation curve, the results disclose that obfuscation operation almost brings no degradation. Figure 11 shows that the packet delay added by security operations is no more than 20 ns.

In fact, the performance drop can only be attributed to the MAC calculation. Although we calculate every verification key based on a master key, the host ID, and the HKDF algorithm to keep stateless verification on host ID, the sampling operation is not conducted on every packet. Therefore, key derivation will not bring much impact. Similarly, the performance of MAC operations can also be improved by using lightweight cryptographic algorithms, hardware acceleration, and shorter input. According to our knowledge, some routers with similar cryptographic functions have achieved line-rate packet forwarding performance by adopting hardware acceleration.

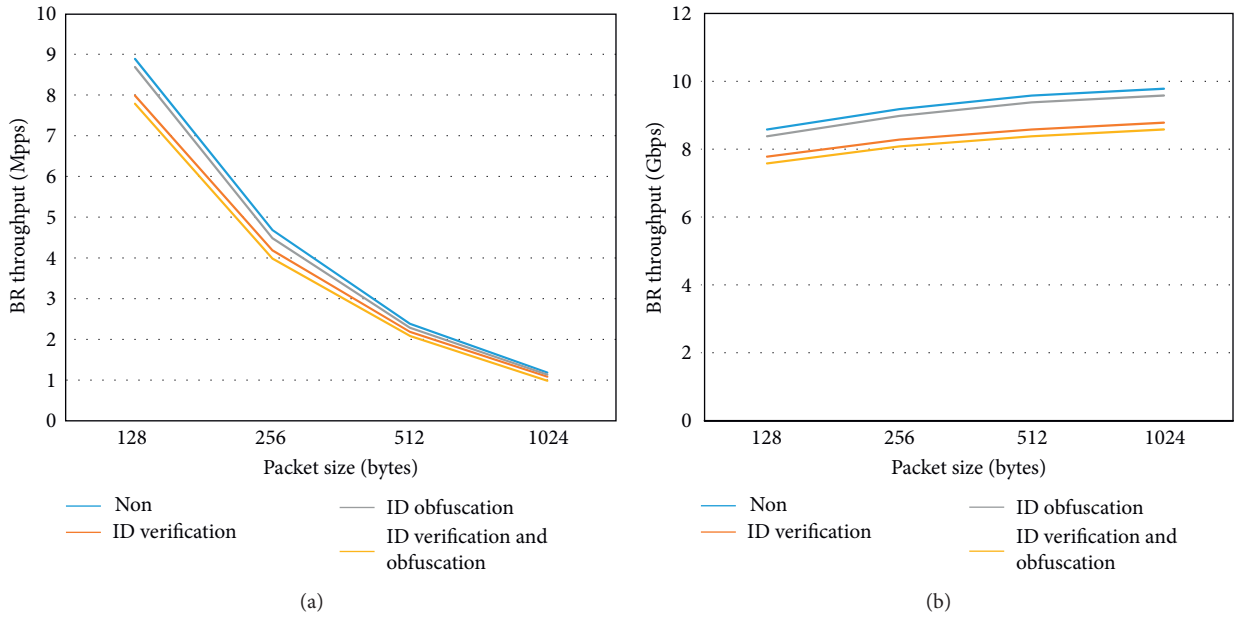


Figure 10: Forwarding performance of the border router expressed as (a) packet rate and (b) bit rate.

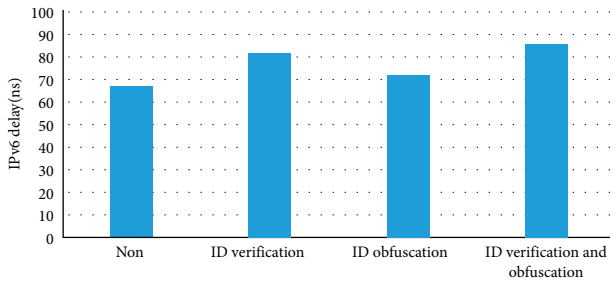


Figure 11: Packet delay on the border router.

6. Conclusion and Discussion

In this article, we analyze the security issues of end-to-end communication and conclude several necessary security requirements for constructing trustworthy networks. We present four key security techniques of NAIS. By isolating ID and locator from IP addresses, we well balance authenticity, privacy, and accountability. The privacy identifiers in the IP header can efficiently prevent cross-site and cross-time slice correlation analysis. The privacy of source location is also preserved without sacrificing routing performance. By deploying multistep verification, we can efficiently prevent spoofing attacks and achieve fast tracing ability. Confidentiality and integrity of packets can also be achieved by providing decentralized public key databases, which can eliminate risks from man-in-the-middle attacks and single point failures. To solve the stubborn DDoS issue, we design three-level defense mechanism, which can greatly enhance network security defense capabilities. Finally, we evaluate the effect of security functions on the packet forwarding performance. The results show that the added security operations will not degrade the performance of the devices in the data plane. Beyond the scope of this article, we will continue to research the motivation mechanism to promote inter-domain collaboration and near-source defense.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] CAIDA, State of IP Spoofing, 2021, https://spoofer.caida.org/summary.php.

[2] X. Chen, W. Feng, Y. Ma, N. Ge, and X. Wang, "Preventing DRDoS attacks in 5G networks: a new source IP address validation approach," in *Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1–6, IEEE, Taipei, Taiwan, December 2020.

[3] NETSCOUT Systems, Netscout Threat Intelligence Report, 2021, https://www.netscout.com/threatreport.

[4] AWS Shield, "Threat landscape report -q1 2020," Technical report, Amazon, Seattle, WA, USA, 2020.

[5] R. Vishwakarma and A. K. Jain, "A survey of DDOS attacking techniques and defence mechanisms in the IOT network," *Telecommunication Systems*, vol. 73, no. 1, pp. 3–25, 2020.

[6] P. Ferguson, "Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing," Technical report, RFC 2827, May 2000.

[7] F. Baker and P. Savola, "Ingress filtering for multihomed networks," Technical report, RFC 3704, March 2004.

[8] A. Bremler-Barr and H. Levy, "Spoofing prevention method,"vol. 1, pp. 536–547, in *Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and*

Communications Societies, vol. 1, pp. 536–547, IEEE, Miami, FL, USA, March 2005.

[9] C. Jin, H. Wang, and K. G. Shin, "Hop-count filtering: an effective defense against spoofed DDOS traffic," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, pp. 30–41, ACM, Washington, DC, USA, October 2003.

[10] F. Lichtblau, F. Streibelt, T. Kruger, P. Richter, and A. Feldmann, "Detection, classification, and analysis of inter domain traffic with spoofed source IP addresses," in *Proceedings of the 2017 Internet Measurement Conference*, pp. 86–99, ACM, London, UK, November 2017.

[11] J. Wu, J. Bi, M. Bagnulo, F. Baker, and C. Vogt, "Source address validation improvement (savi) framework," Technical report, RFC 7039, October 2013.

[12] J. Wu, J. Bi, X. Li, G. Ren, K. Xu, and M. Williams, "A source address validation architecture (SAVA) testbed and deployment experience," Technical report, RFC 5210, June 2008.

[13] T. Ehrenkranz and J. Li, "On the state of IP spoofing defense," *ACM Transactions on Internet Technology*, vol. 9, no. 2, pp. 1–29, 2009.

[14] B. Wu, K. Xu, Q. Li et al., "Enabling efficient source and path verification via probabilistic packet marking," in *Proceedings of the 2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS)*, pp. 1–10, IEEE, Banff, AB, Canada, June 2018.

[15] X. Liu, A. Li, X. Yang, and D. Wetherall, "Passport: secure and adoptable source authentication," in *Proceedings of the 5th USENIX Security Symposium NSDI*, San Francisco, CA, USA, April 2008.

[16] B. Raghavan, T. Kohno, A. C. Snoeren, and D. Wetherall, "Enlisting ISPS to improve online privacy: IP address mixing by default," in *Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium*, pp. 143–163, Springer, Seattle, WA, USA, August 2009.

[17] D. Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms," in *Secure Electronic Voting*, pp. 211–219, Springer, Berlin, Germany, 2003.

[18] S. Paul, D. Roger, and N. Mathewson, "Tor: the second generation onion router," in *Proceedings of the Usenix Security Symposium*, pp. 303–320, San Diego, CA, USA, August 2004.

[19] V. Liu, S. Han, A. Krishnamurthy, and T. Anderson, "Tor instead of IP," in *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, November 2011.

[20] A. K. Jadoon, W. Iqbal, M. F. Amjad, H. Afzal, and Y. A. Bangash, "Forensic analysis of tor browser: a case study for privacy and anonymity on the web," *Forensic Science International*, vol. 299, pp. 59–73, 2019.

[21] J. Hiller, P. Jan, M. Dahlmanns, H. Martin, A. Panchenko, and K. Wehrle, "Tailoring onion routing to the internet of things: security and privacy in untrusted environments," in *Proceedings of the 2019 IEEE 27th International Conference on Network Protocols (ICNP)*, pp. 1–12, IEEE, Chicago, IL, USA, October 2019.

[22] F. Rochet, W. Ryan, A. Johnson, P. Mittal, and O. Pereira, "Claps: client-location-aware path selection in tor," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 17–34, Virtual Event, USA, November 2020.

[23] D. Meyer, L. Zhang, K. Fall et al., "Report from the IAB workshop on routing and addressing," Technical report, RFC 4984, September 2007.

[24] F. Gont, "A method for generating semantically opaque interface identifiers with ipv6 stateless address autoconfiguration (SLAAC)," Technical report, RFC 7217, April 2014.

[25] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic host configuration protocol for ipv6 (dhcpv6)," Technical report, RFC 3315, July 2003.

[26] O. von Wesendonk, "Accountable internet protocol. Innovative internet technologies and mobile communication (IITM)," 2010.

[27] D. Naylor, M. K. Mukerjee, and S. Peter, "Balancing accountability and privacy in the network," in *ACM SIGCOMM Computer Communication Review*, vol. 44, pp. 75–86, ACM, New York, NY, USA, 2014.

[28] T. Lee, C. Pappas, D. Barrera, P. Szalachowski, and P. Adrian, "Source accountability with domain-brokered privacy," in *Proceedings of the 12th International on Conference on emerging Networking Experiments and Technologies*, pp. 345–358, ACM, Irvine, CA, USA, December 2016.

[29] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[30] R. C. Merkle, "Secure communications over insecure channels," *Communications of the ACM*, vol. 21, no. 4, pp. 294–299, 1978.

[31] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[32] D. AdrianK. Bhargavan et al., "Imperfect forward secrecy: how diffie-hellman fails in practice," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 5–17, Denver, CO, USA, October 2015.

[33] N. Li, "Research on Diffie-Hellman key exchange protocol," in *Proceedings of the 2010 2nd International Conference on Computer Engineering and Technology*, vol. 4, p. 634, IEEE, Chengdu, China, April 2010.

[34] L. Dykcik, L. Chuat, P. Szalachowski, and P. Adrian, "Blockpki: an automated, resilient, and transparent public-key infrastructure," in *Proceedings of the 2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, pp. 105–114, IEEE, Singapore, November 2018.

[35] M. Antonakakis, T. April, M. Bailey et al., "Understanding the mirai botnet," in *Proceedings of the 26th Usenix Security Symposium*, pp. 1093–1110, Vancouver, BC, Canada, August 2017.

[36] D. Jiang and G. Liu, "An overview of 5g requirements," in *5G Mobile Communications*, pp. 3–26, Springer, Berlin, Germany, 2017.

[37] Y. Abraham, P. Adrian, and D. Song, "Stackpi: new packet marking and filtering mechanisms for DDOS and IP spoofing defense," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 10, pp. 1853–1863, 2006.

[38] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, Article ID 1550147717741463, 2017.

[39] K. R. W. V. Bandara, T. Abeysinghe, A. Hijaz et al., "Preventing DDOS attack using data mining algorithms," *International Journal of Scientific and Research Publications*, vol. 6, no. 10, p. 390, 2016.

[40] G. Ajeetha and G. Madhu Priya, "Machine learning based DDOS attack detection,"vol. 1, pp. 1–5, in *Proceedings of the 2019 Innovations in Power and Advanced Computing Technologies (i-PACT)*, vol. 1, pp. 1–5, IEEE, Vellore, India, March 2019.

[41] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IOT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[42] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDOS attacks using artificial neural networks," *Neurocomputing*, vol. 172, pp. 385–393, 2016.

[43] M. Jared, M. Schuchard, Routing around congestion: defeating ddos attacks and adverse network conditions via reactive BGP routing," in *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP)*, pp. 599–617, IEEE, San Francisco, CA, USA, May 2018.

[44] C. Dietzel, A. Feldmann, and T. King, "Blackholing at ixps: on the effectiveness of ddos mitigation in the wild," in *Proceedings of the International Conference on Passive and Active Network Measurement*, pp. 319–332, Springer, Heraklion, Greece, March 2016.

[45] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "Ddos attack protection in the era of cloud computing and software-defined networking," *Computer Networks*, vol. 81, pp. 308–319, 2015.

[46] K. Seyed, Y. Tobioka, V. Sekar, and M. Bailey, Bohatei: flexible and elastic DDOS defense," in *Proceedings of the 24th Usenix Security Symposium*, pp. 817–832, Washington, DC, USA, August 2015.

[47] T. Reddy, M. Boucadair, P. Patil, A. Mortensen, and N. Teague, "Distributed denial-of-service open threat signaling (DOTS) signal channel specification: internet-draft," 2018.

[48] A. Bernard, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz et al., "Extensible authentication protocol (EAP)," Technical report, 2004.

[49] IEEE Standards Association, "802.1x-2020-IEEE standard for local and metropolitan area networks–port-based network access control," 2020.

[50] J. LarischD. Choffnes et al., "Crlite: a scalable system for pushing all TLS revocations to all browsers," in *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP)*, pp. 539–556, IEEE, San Jose, CA, USA, May 2017.

[51] Y. Liu, W. Tome, L. Zhang et al., "An end-to-end measurement of certificate revocation in the web's PKI," in *Proceedings of the 2015 Internet Measurement Conference*, pp. 183–196, ACM, Tokyo, Japan, October 2015.