7-2016

A survey on future internet security architectures

Wenxiu DING
Xidian University

Zheng YAN
Aalto University

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 22, 2016, accepted July 8, 2016, date of publication July 29, 2016, date of current version August 26, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2596705

A Survey on Future Internet Security Architectures

WENXIU DING[1], ZHENG YAN[1,2], (Senior Member, IEEE), AND ROBERT H. DENG[3], (Fellow, IEEE)

[1]State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China
[2]Department of Communications and Networking, Aalto University, Espoo 02150, Finland
[3]School of Information Systems, Singapore Management University, Singapore 178902

Corresponding author: Z. Yan (zhengyan.pz@gmail.com)

This work was supported in part by the National Key Foundational Research and Development on Network and Space Security, China, under Grant 2016YFB0800704, in part by NSFC under Grant U1536202, in part by the 111 Project under Grant B08038, in part by the Ph.D. Chinese Educational Ministry under Grant JY0300130104, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Program 2016ZDJC-06, and in part by Aalto University.

ABSTRACT Current host-centric Internet Protocol (IP) networks are facing unprecedented challenges, such as network attacks and the exhaustion of IP addresses. Motivated by emerging demands for security, mobility, and distributed networking, many research projects have been initiated to design the future Internet from a clean slate. In order to obtain a thorough knowledge of security in future Internet architecture, we review a number of well-known projects, including named data networking, Content Aware Searching Retrieval and sTreaming, MobilityFirst Future Internet Architecture Project (MobilityFirst), eXpressive Internet Architecture, and scalability, control, and isolation on next-generation network. These projects aim to move away from the traditional host-centric networks and replace them with content-centric, mobility-centric, or service-centric networks. However, different principles and designs also raise various issues on network security. For each project, we describe its architecture design and how it deals with security issues. Furthermore, we compare these projects and discuss their pros and cons. Open security issues are pointed out for directing future research.

INDEX TERMS NDN, COAST, MobilityFirst, XIA, SCION, future internet, security.

I. INTRODUCTION

The current Internet designed 40 years ago has evolved from an academic network to a widely used commercial network. It has been deeply involved in our daily life and become an indispensable part of our society.

Internet began with packet switching for military requirement [1]. As the Internet evolved, Transmission Control Protocol/Internet Protocol (TCP/IP) was adopted in 1980. The IP as a principal communication protocol in Internet Protocol Suite (IPS) has the task of delivering packets from a source host to a destination host solely based on IP addresses. To realize data transmission, the IP defines its format of packets that includes a header and a payload. The IP header is tagged with the source and destination IP addresses that identify hosts and provide a logical location service. Internet Protocol Version 4 (IPv4) [2] is the first publicly used version of the IP and is still the dominant protocol of the current networks. But the 32-bit address applied in IPv4 restricts address space, which makes it hard to identify various hosts with the fast growth of the Internet and to support future development. In order to solve this problem, Internet Protocol Version 6 (IPv6) [3], which is intended to replace IPv4 [4], is designed with 128-bit address yielding 3.4×10^{38} addresses and specifies a new packet form. General worldwide deployment of IPv6 is increasing. For example, the percentage of top level domains with IPv6 name servers has achieved 97.9% [5] and the percentage of users that access Google over IPv6 has increased to 12% [6].

Although the IP protocol achieves great success and is widely used, it still triggers many challenges to the network. First, a host-centric IP network does not conform to highly distributed communications. The sustained growth in e-commerce, digital media and social networking has led to the dominant use of the Internet as a distributed network. However, each packet transmitted over the Internet with a host-centric design principal needs information about its destination and its source (i.e., IP), which limits the development of distributed networks. Second, the Internet connects billions

of nodes and even more in the future, which will mostly suffer from the exhaustion of IP addresses, especially IPv4 addresses [7]. Third, the current Internet is absent of security design in its original architecture and is hindered by more and more sophisticated network attacks. Though IPv6 extends the address space and offers globally unique IP addresses to enhance security (e.g., authentication), it still faces many other security issues [8], [9], such as flooding issues and mobility issues. Some new protocols (e.g., IPSec [10] and DNSSec [11]) have been designed to complement the existing protocols, but they still have security weakness (e.g., clogging system) [12]. However, the involved entities nowadays pay much attention to security, scalability, and mobility and so on in social life, especially economic activities. Security is expected to be embedded in the network design as an inherent feature. Fourth, it is difficult to add new functionalities and new usage models into the current Internet architecture to satisfy its increasing new demands. Because current methods for incremental deployment always involve tunnels or overlays, which easily hide the new functionality from the existing network. For example, if some entities are intended to support content-centric networking with a tunnel, then the traffic that ends up being tunneled through the network using IPv4 would still need source and destination addresses. The features of content-centric network cannot be fully presented. The emergence of new needs makes its original functionalities (e.g., storage, transmission, etc.) under pressure [13], while most of patches are temporal solutions and increase the complexity of architectures [14]. In general, the inconsistency between the Internet design and real usage demands urgently calls for a clean-slate Internet architecture.

There have been significant research efforts on the topic of Future Internet Architecture (FIA), which aims to overcome the above challenges, and security has become an indispensable part and been taken into consideration seriously in these architecture designs. These efforts are widely made all over the world, e.g., in the Unites States and the European Union (EU). However, security as a complex problem brings many challenges, which are difficult to be covered by any single project. In this paper, we survey five famous projects of FIAs, which are based on various principles. Different from some existing surveys [15]–[17], our work focuses on the security requirements and potential countermeasures, which play a baseline of future security work in this area.

Information-Centric Networking (ICN) has emerged as a promising candidate for FIA design. The NDN project [18]–[20] as a derivative ICN work was funded by the U.S. National Science Foundation (NSF) under its FIA Program [21]. This new Internet architecture moves from typical host-centric to content-centric one and focuses on what- the content rather than where- the addresses and hosts, which further develops the Content-Centric Networking (CCN) architecture [22]. It adopts the hourglass architecture derived from the success and lesson of today's Internet, and proposes to cache the content in routers, which can reduce network traffic. However, it also introduces new issues, especially efficient signature and trust management problem.

Another content-centric network, COAST [23], [24] was within the European Research Program 7 [25] and partially funded by the European Commission. It builds an overlay architecture, which aims to find desired data in the closest networking devices and forward it to a data consumer as fast as possible. In contrast to the NDN, the COAST implements intelligent routers and nodes in an overlay network, which can monitor and filter traffic flows and verify transmitted contents in the network in order to enhance security.

As the name indicates, MobilityFirst [26]–[29] was designed with mobility as a crucial top-level design goal, which was also conducted as part of the FIA program under NSF. The MobilityFirst adopts a massive Global Name Resolution Service (GNRS) to dynamically bind names and addresses to achieve mobility and enhance security.

Yet another NSF project, XIA [30]–[32] designed a clean-slate network architecture to achieve several goals: trustworthiness, long-term evolution of usage models, long-term technology evolution and explicit interfaces between network actors. Besides the content principal in the NDN and the COAST and the host principal in current networks, the XIA also supports many other principals (e.g., networks and services including transport protocols and mobility services) and even new ones emerging in the future.

Finally, SCION [33]–[35] was designed with the ability to provide route control, failure isolation and explicit trust information for end-to-end communications. It adopts the notions of Isolation Domains (ISDs), Autonomous Systems (ASes) and Trust Root Configuration (TRC) to deal with routing and trust management. The SCION can achieve high availability even in the presence of distributed adversaries and resist some existing popular attacks. Patch Construction Beacons (PCBs) were introduced to discover and establish routing paths.

Contributions of this paper can be summarized as below:

- We provide a thorough overview of the above five projects, including their principles and special features, especially security concerns and countermeasures.
- We present the pros and cons of each project, and compare the five projects in terms of security properties.
- We further discuss the security issues that should be taken into consideration in the design of future Internet architecture.
- We propose some open issues to guide the future research.

The rest of the paper is organized as follows. The NDN is presented in Section 2, followed by the COAST that is reviewed in Section 3. Section 4 discusses the MobilityFirst. Then the XIA and the SCION are presented in Section 5 and Section 6 respectively. The pros and cons of the five projects and their comparison are given in Section 7, followed by further discussions on future research issues in Section 8. Finally, a conclusion is presented in the last section.

II. NAMED DATA NETWORKING (NDN)

The current Internet Protocol (IP) was designed to create communications between a source and a destination that are identified by IP addresses. However, it is not applicable to highly distributed networks. What users really care about is what they get rather than where it is from. Therefore, the NDN project [18]–[20] was proposed to overcome the weakness of the Internet's current communication architecture and accommodate emerging patterns of communications, which shifts its point from where- the host to what- the content. Similar to current IP architecture, the NDN has its own narrow waist design. But it uses data names instead of IP addresses for delivery, which removes the restriction of the length of IP addresses and enables scalable communications.

In this section, we give a brief description of its architecture and introduce the solutions proposed by the NDN to fulfill its specified security requirements.

A. NDN ARCHITECTURE

The NDN is a new architecture, grounded in current practice. Some basic architectural principles are described as follows:

- **Hourglass Architecture**: The NDN remains the hourglass-shaped architecture of IP architecture, but makes some revisions. Specially, it replaces IP packets with content chunks.
- **Security:** Decoupling data from how or where it is obtained and signing all Data packets provide effective ways to ensure data trust [36]. The signature also guarantees data integrity and enables verification on data provenance.
- **End-to-End Principle:** The NDN keeps this principle because of its good performance to enable development of robust applications in the face of network failures.
- **Self-Regulating Network Traffic:** To make the Internet stable, the NDN incorporates traffic-flow-balance.
- **Routing and Forwarding Plane Separation:** the NDN adopts this principle to allow its deployment with the best available forwarding technology while carrying out new routing system research in parallel.

In the NDN, the receiving endpoint, i.e., a data consumer, drives communications. Two kinds of packets are transmitted through the Internet: Interest and Data. A consumer sends an Interest packet indicating its desired data with a name to the network, and then routers forward the Interest packet towards any producers (i.e., data sources). If the Interest packet reaches a node that has the desired data, the node then returns a Data packet containing both the same name as specified in the Interest packet and the required content. The Data packet needs to be signed to enhance security. This Data packet follows in reverse the path to get back to the requesting consumer.

In the following subsection, we present the details of each element in the NDN architecture.

1) NAMES AND ADDRESSES

Names in the NDN play the same role as the target and source addresses in IP, which guide the forwarding and routing of the Interest packets and Data packets. Owing to the opaqueness of names, a router can organize the boundaries between components in names without knowing the meaning of the name. For example, a video produced by Singapore Management University (SMU) may have the name /smu/videos/demo.mpg, where '/' delineates the name components similar to URLs. The NDN names are opaque to the network [18], [19] and are designed in hierarchical structure.

To dynamically retrieve desired data, data consumers must be able to deterministically construct the name of their desired data before they get to know their contents. Two methods can be applied: (1) A deterministic algorithm can arrive at the same name based on the information available to both data producer and consumer; (2) Retrieve the desired data through one or more iterations depending on the Interest selectors and longest prefix matching [37], [38]. The data reachable globally must have globally unique names, but those names for local communications can be based on local context because it only requires local routing to search for desired data.

Namespace management is not regarded as a part of the NDN architecture, hence the concrete design of names is not considered, especially the opaqueness. However, naming is the most important part of the architecture which is the basis of all other functionalities (e.g., data acquisition and data distribution), and its structure is highly related to security [39]. Efficient management of names is of great significance in the development of the NDN, especially the opaqueness design of names.

2) CACHING

Independent of who requests or from where it is retrieved, the NDN Data packet can be cached in the router's Content Store (CS) opportunistically. Once receiving an Interest packet, the router first checks if the desired data has been stored in its CS. If yes, the Data packet can be sent back directly to the data consumer. Thus, the data consumer may obtain the desired data even before the Interest packet reaches the data producer(s). The caching exhibits the superiority over IP in data delivery, multicast and even retransmission after a packet loss.

The NDN tries to enhance privacy by only specifying the name of desired data. This works differently from the traditional Internet, where one can find out what is in the packet and who is requesting the data by checking the header or payload of a packet in the IP network. But the caching of Data packets in routers also incurs many privacy issues that retard the deployment of the NDN, which are discussed in Section 2.2.

3) ROUTING AND FORWARDING

The NDN routes and forwards packets based on names rather than addresses, which eliminates some serious problems in the IP architecture: 1) the exhaustion of address space; 2) Network Address Translation (NAT) traversal problem; 3) address assignment and management problem.

To forward the Interest and Data packets successfully, each NDN router maintains three data structures: a Pending Interest Table (PIT) for storing all the Interests that a router has received but not satisfied yet, a Forwarding Information Base (FIB) for making informed decision about how to deal with the Interest packet flexibly, and a Content Store (CS) for opportunistically storing Data packets.

When an Interest packet carrying a data name arrives, the router needs to check its own data structures to complete forwarding process as following:

a) It first checks if the required data has been cached in the CS. If yes, the Data packet can be sent back directly. Otherwise, step to b).
b) It further looks up this name in its PIT entry. If a matching Interest record exists in the PIT (that is, the router has forwarded the Interest packet), it simply adds the incoming interface to the PIT entry and waits for the Data packet. The router only needs to forward the first Interest packet if it receives the same Interest packets more than once from different nodes. Otherwise, step to c).
c) The forwarding strategy module together with FIB information makes the informed decision about how to deal with the Interest packet flexibly. Then the router completes its forwarding process according to the decision. For example, if the upstream link is down or extremely congested, the router can send a Negative Acknowledgement (NACK) to its downstream neighbors, which may trigger other router to explore other routes to forward the Interest. It can finally mitigate congestion and resist potential DoS attacks.

When the Data packet arrives, the forwarding procedure is much simpler. The router first looks up the Interest packet with the same name in its PIT entry. If no record exits, it directly discards the Data packet; Otherwise, it forwards the Data packet as a response, then removes the record from the PIT. If a timeout occurs, the Interest record will also be removed from the PIT. In addition, the Data packet can be cached opportunistically in the CS for a period of time, which leads to an efficient network without the need for any notion of source or destination nodes in data delivery.

Additionally, applying the PIT in the NDN design has some other advantages:

1) The PIT enables multicast data deliveries according to its Interest record. When the Data packet arrives, the router can multicast it to related interfaces stored in the PIT.
2) The self-control of the number of pending Interests results in a flow balance. Each Interest retrieves at most one Data packet, but a router needs to forward the Data packet to all requesters. If a router is overloaded, it can autonomously choose to slow down or stop pending Interest packets in the PIT.
3) The control on the number of PIT entries can constrain the effect of a DDoS attack. If a router receives the same Interest packet it has forwarded, it has no need to forward it again. Meanwhile it controls the number of Interests for different Data packets, which also controls traffic loads. Thus it constrains the influence of DDoS attacks on the network.
4) The timeout record of the PIT entry can help detect attacks. If an Interest packet is kept in the PIT overtime and the router does not receive its corresponding Data packet, then the router can mark the source of the Interest packet as a suspicious attacker. Especially, if one timeout Interest packet is always transmitted over the network, it is probably a DoS attack.

B. SECURITY IN NDN

The NDN architecture takes the security into consideration during the design and aims to resist some popular types of Internet attacks. However, it also poses some new problems. In this section, we will focus on security issues that the NDN solves and triggers.

1) DoS & DDoS AND COUNTERMEASURES IN NDN

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) threaten the Internet in recent years. The adversary in DDoS exploits a huge number of compromised machines or zombies to attack a specific target. The DDoS attack is easy to execute and difficult to be mitigated. Therefore, it is crucial to limit or even eliminate the effects of the DDoS attack.

In the NDN architecture, the Data packet is only delivered upon a request and the Interests for same data are merged into one Interest packet. Moreover, the number of PIT entries and the timeout record can be used to analyze and detect attack behaviors. This pull-model can effectively eliminate some existing DDoS attacks.

However, two new types of NDN-specific DoS attacks towards the new architecture were identified by Gasti [40]: interest flooding and content/cache poisoning.

a: INTEREST FLOODING

As the router needs to store Interest packets in the PIT, it is possible for an adversary to send a huge number of Interest packets to flood a particular data producer or overflow the PITs, which leads to the failure of handling legitimate Interest packages. The requested contents by adversaries can be classified into three types: existing static contents, dynamically-generated contents and non-existent contents. Correspondingly, the Interest flooding attack towards each type of content has different effects:

- Existing static content: NDN has a built-in countermeasure that caches the Data packet.

Therefore, NDN routers do not forward subsequent Interest packets for the same existing content.

- Dynamically-generated content: In this case, all Interest packets are routed to data producer(s), thus they consume network bandwidth and the PIT of routers, thus inducing intrusions.
- Non-existent content: The router can immediately remove an invalid request, but this attack can still affect the PIT by occupying its storage space as they will be stored until they expire.

Regarding to these attacks, Gasti et al. proposed two potential countermeasures:

- Router Statistic: NDN routers keep track of the expired Interest packets and set a threshold to the pending Interest packets. They limit: the number of pending Interest packets per interface; the number of Interest packets per interface; and the number of pending Interest packets per namespace.
- Push-back Mechanisms: The goal of push-back mechanism is to isolate attack source. Once a router suspects an on-going attack from one interface, it will report to the routers close to the interface. Iteratively, these routers will send the reports towards the offending interface where the suspicious attack comes from and finally push back to its source.

Compagno et al. [41] further pointed out the weakness of these countermeasures and further proposed to mitigate the attacks in an initiative way from the perspective of detection and reaction.

b: CONTENT/CACHE POISONING

The adversary targets data contents and causes the router to forward and cache corrupted data. Generally, it compromises the NDN routers. When the Interest packet arrives, the compromised router will return the poisoned Data packets.

To counteract this type of attack, the involved parties apply self-certifying Interest and Content or Collaborative verification techniques. The countermeasure can verify the association between a name and a corresponding content, and the validity of the content. An alternative is to utilize smart forwarding to mitigate the caching poisoning attack [42]. If receiving a bad Data packet, an Interest packet that contains an indication to exclude the poisoned content can be sent to notify its upstream router.

2) DATA SECURITY AND PRIVACY ISSUES IN NDN

Signing Data packets not only guarantees data integrity, but also realizes a certain level of trust. It allows the consumers to reason whether a data producer is acceptable for providing particular data in a specific context. However, trust between consumers and producers could be dynamically changed, which makes it hard to adopt a ''one fits all'' trust model. Hence, the NDN should figure out a set of usable trust mechanisms for a wide application range, which needs further experiments and investigation. An example of trust management is described in [43]. All the potential advantages of the NDN rely on an efficient digital signature system and effective trust management. But key revocation and management are still open and crucial issues.

In addition, the NDN is innate privacy-friendly due to lack of source and destination in terms of their network addresses. But it still prompts some privacy concerns stemming from the semantic richness of names and data privacy besides the problem above. The names used for retrieving contents are semantically related to the contents themselves. An attacker could infer sensitive information about a user, by monitoring its requests. Thus, content name opaqueness becomes a very urgent research issue. Bloom filter [44], [45] may be a possible technique to deal with this problem. Moreover, digital signatures of Data packets need to be publicly verifiable; hence the identity of a content signer may be easily inferred by looking at the signature. DiBenedetto et al. [46] proposed to enhance the privacy with anonymity. It introduces a pair of distinct anonymizing routers to realize the routing with encrypted Interest packet.

As described in Section 2.1, the cache of Data packet exhibits great superiority in data delivery. Once the desired data has been stored, the data consumer can obtain it in almost optimal speed with lowest network traffic. Owing to the names of data, the retrieve of content fragment is much easier than that in the current network with caching on the routers [47]. Caching in the NDN helps reduce congestion, improve delivery speed, and optimize bandwidth consumption. But this feature also reflects some potential issues of damaging the privacy of data consumers and producers [48], [49]. One of the most serious problems is data confidentiality. Data packets cached at routers are available to anyone that requires for them, which is exposed to data leakage. Many cryptographic techniques (e.g., symmetric encryption, broadcast encryption, Proxy Re-Encryption (PRE), etc.) and access control mechanisms [50], [51] can be potentially used to protect the data. But they incur many other problems, such as disabling caching mechanism, and extra computation and communication overhead. The NDN still seriously lacks a practical scheme to guarantee data security. Beside content confidentiality, responses at routers with caching could also intrude user privacy. For example, one consumer forwards its Interest packet for one specific data. If he/she obtains the data very fast, then he/she can be sure that someone nearby has received the same data. Thus, it obliviously exposes some information to subsequent consumers, which may be unacceptable in some sensitive scenarios. In order to protect the privacy of data consumers, Acs et al. [48] proposed some methods to overcome this weakness. As not all contents are private, then it is possible to specify which content is sensitive. The data producer, the consumer or both of them can drive it. Some techniques were proposed to provide certain tradeoffs between privacy and latency and inhibit adversaries from extracting meaningful information from the traffic via router caches. Chaabane et al. [49] pointed out the privacy problems about caches, contents, names and signatures existing in the content-centric networking. They also proposed

several countermeasures to overcome the flaws caused by monitoring or censorship, such as waiting before replying, encrypting data, bloom filters, and group signatures, etc.

In general, data security and privacy preservation are vital in the development and employment of the NDN architecture in the future.

III. CONTENT AWARE SEARCHING RETRIEVAL AND STREAM (COAST)

The COAST project [24] is a Specific Targeted Research Projects (STREP) project within the European Research Program 7 and partially funded by the European Commission. It also aims to build a content-centric network architecture to intelligently and efficiently link billions of content sources to billions of content consumers, and offer fast content-aware retrieval, delivery and streaming.

In the COAST, the data consumers only need to specify their desired data and then the COAST framework can search and return the data to the consumers efficiently, realizing the Service Level Agreements (SLAs) in content consumption.

A. COAST ARCHITECTURE

Similar to the NDN, the COAST project designed a content-centric architecture, which aims to improve the content discovery and delivery. As mentioned above, current Internet content delivery as the vast majority of Internet usage is based on the IP addresses of the source and the destination. Usually, search engines crawl over the Internet to find, classify and index contents or services for potential use. Once a data consumer queries a search engine, it will get a number of URLs related to the desired content. Finally, the consumer selects a URL to access the data.

However, the data access procedure is inconsistent with real usage. For example, two data consumers close to each other require for a famous video from YouTube. The video will be streamed a few dozens of times per square blocks to the two consumers respectively. The same data must have been flowed through the same routers twice to reach the neighbor consumers. But in real usage, the data can be transmitted through the longest common path before bifurcating the same message to the two neighbor consumers. The COAST aims to eliminate the inconsistency above and adapt to the real usage. The same data do not need to be flowed multiple times through almost the same paths in the COAST. The COAST is a multi-layer network and consists of various virtual hierarchies of nodes with different functionality. An example design of three layers [24] is presented as follows:

1) THE LOWER LAYER - NETWORK PROVIDER INFRASTRUCTURE OVERLAY

This layer is the infrastructure of Internet Service Provider (ISP) and network providers, which also includes some nodes with limited functionality and intelligence. Users are considered as Content Producers and Consumers, and content is routed via this layer.

2) THE MEDIUM LAYER - DISTRIBUTED CONTENT/ SERVICES AWARE OVERLAY

Content-Aware Network Nodes (e.g., edge routers, home gateways and terminal devices) in this layer have the intelligence to filter the content and service flowing through them, identify streaming sessions and traffic, and finally provide qualification for the legitimate content. The qualification will be reported to the higher layer of hierarchy. Additional functionalities can be added by constructing virtual overlays at this layer. The nodes can operate as hybrid client-server and/or P2P networks, according to delivery requirements.

3) THE HIGHEST LAYER - INFORMATION OVERLAY

This layer consists of intelligent nodes or services that have a distributed knowledge of content/web-service location/caching and network instantiation/conditions. This layer makes decisions on the way to optimally retrieve and distribute data to consumers or inquiring users or services, which is based on its awareness of the content/services location/caching over the network and related network information. The content may be stored/cached at the Information Overlay or at the lower hierarchy layers.

a: DISTRIBUTED CONTENT AND SERVICE SEARCHING

To achieve better performance, the COAST aimed to design solutions for crawling, indexing and query processing that can take the full advantage of multiple distributed sites (including nodes, sites, and data centers). The COAST presents two ways to perform crawling:

- Active Crawling: Crawlers fetch documents from the Internet, index their information, and follow links in this fetch.
- Passive Crawling: The search engine receives indexable information out of Deep-Packet Inspection (DPI) performed by the COAST intelligent nodes in the medium layer. Intelligent nodes scrape data, cache them and send interesting contents and new services to the Information Overlay.

However, an efficient discovery mechanism needs to be designed and verified.

b: CACHING

Like the NDN, the COAST also adopts content cache to increase network efficiency and lower data delivery delay. But it caches data contents, query results and parts of indexes. And it caches these data not only at the highest layer, but also at the intelligent nodes of the medium layer. The intelligent nodes of the highest layer also cache contents, while the search engine maintains information about the caches copies. It can guide the data consumers to the closest cached copies with the cooperation of intelligent nodes and the search engine.

c: CONTENT-AWARE DELIVERY

To achieve a smooth delivery of media contents, the medium layer collects and exploits the information available in the COAST to organize, optimize and deliver the contents.

Content-aware delivery is enabled by four key factors as described below.

- Distributed media identification: The COAST performs distributed media storage through content indexing/caching services to define a distribution policy and optimally route content distribution.
- Content-aware probing: The COAST optimizes and performs actual content delivery processes. The better awareness of the content it obtains, the better delivery policy it defines. Therefore, it firstly needs to define a set of metrics, a simple model to estimate the PQoS (Perceived Quality of Service) and estimate the performance of the overlay at a global level, thereby estimating the available delivery policies for new sessions.
- Matching content and network: The types of contents, their current availability and locations, their characteristics and even the features of the content representations will be taken into consideration.
- Content-aware streaming: The streaming process will be based on bandwidth-efficient and low-delay strategies to improve delivery performance. In P2P, every peer node should know the relationships between its peers and the segments of desired data to fetch the desired segments correctly.

B. SECURITY IN COAST NETWORKS

Both the NDN and the COAST are content-centric rather than host-centric, but they differ in security. All packets including Interest packets and Data packets are verified and filtered in the COAST while only the Data packets are verified in the NDN. As a content-centric architecture, the COAST avoids some attacks towards the host-centric IP networks, but it is exposed to some new attacks.

1) DoS AND DDoS IN COAST NETWORKS

Similar to the NDN, the COAST also applies the cache to gain better performance in data delivery. As a result, it may be exposed to COAST-specific DoS/DDoS attacks besides the traditional DoS/DDoS attacks.

Fortunately, the COAST incorporates basic defenses in its design. The network nodes in the Distributes Content/Services Aware Overlay have intelligence to filter contents and Web services, and offer qualification for legitimate contents. With the capability to add virtual overlays at this layer, the COAST would be able to monitor and detect abnormal streaming. Moreover, the intelligent nodes at the Information Overlay have knowledge of content caching and network instantiation. The intelligence at the two layers can ensure the validity of a data flow and eliminate the caching of contents generated by adversaries. The DoS/DDoS attacks can only dissipate the bandwidth and nodes' time to filter the flow.

2) HOST-OBLIVIOUS NETWORK SECURITY (HONS)

The current network security relies on the operations of network, thus its security systems depend on the host-centric architecture. As pointed out in [52], the content-centric networks cannot apply host-dependent network security schemes. Therefore, a new paradigm named Host-Oblivious Network Security (HONS) was proposed.

The HONS adopts the q-composite Rand Pool-Based (q-RPB) scheme for host-oblivious and mutually independent multiple secure associations [53]. It dynamically changes security association to resist the weakness of a host-based key under key exposure. A Key Distribution Center (KDC) manages a Key Pool (KP). The KDC as a trusted entity shares a symmetric key with each node and is responsible for issuing a Key Ring (KR) for each node. Each key in the KR has its index, which is used for building a session key. When a node requests for data, it forwards an Interest packet, a hashed MAC and a set of index of q-number of keys, etc., the responder validates the information with the same key index. Hence, the responder can generates the session key with the requesting node $K = hash(\{k_i\}^q)$, where k_i is indicated by the key index and q is decided by the security-sensitivity of content. Moreover, neither the data requester nor the data responder has any idea about each other except the host-oblivious keys.

The HONS can achieve confidentiality, integrity, authentication, and source and destination anonymity. But the HONS has a low probability of successfully establishing the session key between a data consumer and a data producer. As stated above, the HONS is applicable to the NDN and the COAST because both of them are content-centric.

IV. MobilityFirst FUTURE INTERNET ARCHITECTURE PROJECT (MobilityFirst)

The MobilityFirst project [26]–[29] was started in 2010 funded by the FIA program under NSF. It is a specific realization of the emerging class of ICN [54]. As the name indicates, the MobilityFirst project was intended to address the problem of mobility. The mobile devices outnumber the tethered Internet hosts. But the current Internet with hardly changed architecture and hosts cannot accommodate to the rapidly increasing number of mobile devices, which drives the design of the MobilityFirst. Furthermore, it was designed with trustworthiness as a goal in mind.

As one of the most important and outstanding designs, a massively scalable name service was adopted to separate the names and network address. Additionally, the Globally Unique Identifier (GUID) was defined to enhance security.

A. MobilityFirst ARCHITECTURE

The current Internet architecture cannot satisfy the demand of network users. There exist a few problems: (1) the Internet cannot resume the download when device moves; (2) the current network is fragile in mobile and wireless network; (3) additional infrastructure is needed to support seamless mobility. In order to address the challenges above, the MobilityFirst designs several key components:

- **Decentralized Name Certification Service (NCS)**: The NCS securely binds human-readable name to

a GUID. The GUID is a cryptographically verifiable identifier, which can improve the trustworthiness and allow seamless mobility. It can be used as a public key to provide a mechanism for authentication and trust management for attached devices or objects. The MobilityFirst can also support context-based descriptor by mapping the context to a particular GUID.

- **Global Name Resolution Service (GNRS)**: GNRS is a central component and responsible for supporting seamless mobility. It securely maps the GUID to a Network Address (NA) if the GUID has been assigned to an object. The cooperation of the NCS and the GNRS can bind a readable name to a network address, which is the base of communications.
- **Computing and Storage Layer**: As an imperative requirement, evolvability is achieved by supporting a computing and storage layer, which can enable rapid introduction of new and possibly niche services without impacting remaining traffic and fast forwarding paths.

1) NAMES AND ADDRESSES

The MobilityFirst separates human-readable names, GUID and network locations. The GUID can be assigned to not only devices but also contents. A content GUID differs a little bit from an interface or device GUID. The self-certifying content GUID is a one-way hash value of the content itself, which allows any entity to check its integrity. Additionally, the GNRS would not save a state for all content GUIDs, which helps reduce the overhead of a GNRS provider. The routable content address will be encoded as a two-tuple of content GUID and producer GUID denoted as [CID, PID]. Then, the data consumers who know the tuple can request for desired data.

The destination GUID is attached to a Packet Data Unit (PDU). Another service identifier in the packet header is used to indicate the type of service, such as unicast, multicast, anycast, context delivery, etc. The first router will resolve the destination GUID and obtain dynamical mapping from the GNRS. The resolved NAs are optionally chosen to guide data forward. A self-certifying GUID can be easily implemented by computing a one-way hash of a public key. And it can be authenticated through a bilateral challenge-response protocol.

To establish a communication with an endpoint GUID, a sender first queries the GNRS about the corresponding NA of GUID and then sends its packets to the destination. Thus, the sender and the receiver can construct their communication based on NAs.

2) CACHING

Similarly, in the NDN and the COAST, the MobilityFirst also takes the advantage of caching to improve network performance. It exploits in-network storage at routers to temporarily store Protocol Data Unit (PDU) that can cope with variations in wireless access network bandwidth and occasional disconnections. Furthermore, a generalized storage-aware routing (GSTAR) protocol [55] can integrate Delay Tolerant Networking (DTN) capabilities to provide a seamless solution. The storage-aware routing can also be used together with block transport to enhance network performance and disruption-tolerance.

3) SCALABLE MOBILITY AND CONTENT-AWARE DELIVERY

Though the GUIDs are fixed, the endpoints are possible to frequently change their network points and result in different NAs. Generally, endpoint mobility falls into four possible cases according to the time an endpoint moves:

1) *Pre-lookup mobility* suffices if the endpoints rarely change their network addresses.
2) *Connect-time mobility* is regarding the scenario that a destination moves before a connection is established but the initiator has queried. The initiator simply relaunches a three-way handshake when its first request timeouts.
3) *Individual mobility* refers to one endpoint moving after a connection has been established. The moved endpoint can directly re-synchronize the communication by sending a message to its peer with its new NA.
4) *Simultaneous mobility* happens when the other endpoint moves in individual mobility but the connection of the endpoints has not been re-synchronized. The endpoints should restart the whole constructing process.

Besides the endpoint mobility as described above, the GNRS also enables network mobility wherein a whole network moves across locations. This feature would be very suitable for ad hoc infrastructure-less communications between mobile devices (e.g., vehicle or body-area networks).

To achieve high scalability, a hybrid name/address is adopted in the MobilityFirst. As the number of forwarding table entries in a core router should be commensurate to the total number of NAs, the Internet routing protocol is designed to support a hierarchy architecture to trade off packet header space against forwarding table size. The core network router only keeps the forwarding entries for other core networks and a few ''consumer'' edge networks; while the edge network router keeps forwarding entries only for a few ''producer'' core networks and edge networks nearby.

Moreover, the MobilityFirst can support content-aware and context-aware services based on multicast. Multicast as an instance of context-aware delivery can be achieved easily. First, a multicast GUID (MID) is introduced. The GNRS maintains the membership set of each MID consisting of all GUIDs belongs to the multicast group. Each member GUID i in MID subscribes to the group via a single home NA. The name service resolves a MID by collecting and returning the union of all NAs ($NA_i, i = 1, \ldots, N$) that have the members subscribing to the MID. A sender would send the data addressed to $[MID, NA_i]$ for all NAs respectively. Finally, NA_i resolves the MID to the subset of GUIDs and forwards the data to each member depending on an intra-network routing protocol. Content-aware delivery is similar

to multicast, which sends data to groups based on attribute-based descriptors. For example, to enable a geo-casting, each potential member should maintain its geolocation attribute. The GNRS creates a context-aware MID to describe the specified geolocation. The sender delivers its data to the members matching this MID, which is similar to the procedure of multicast as described above.

The MobilityFirst also involves the dual-homing service that a device can have two or more wireless interfaces which is hard to handle in the IP protocol. For example, a user's laptop may have two or more wireless interfaces (such as WiFi and 3G) on separate access networks, and the service objective is to deliver to at least one of these interfaces based on a suitable cost metric. The PDU carries these network addresses. A network routing protocol implements a longest common path type of algorithm before bifurcating a same message to both interfaces. The dual-homing service can easily solve the disconnection over a network edge and provide seamless mobility.

In general, the MobilityFirst provides good mobility and scalable routing services, which enhances its performance in various application scenarios.

B. SECURITY IN MobilityFirst NETWORKS

1) SECURITY ROOTED IN MobilityFirst

Different from the hierarchical names in the NDN, the MobilityFirst adopts a globally unique identifier to name devices, interfaces and even contents. The unique identifier can be securely bound to its corresponding entity, which lays the foundation of security and privacy for this project design.

The GNRS is responsible for a massive replication and federation of name certification as well as the name resolution. Therefore, it is vulnerable to DDoS attacks if the adversary tries to exhaust the resource of GNRS. Fortunately, the property of self-certifying GUID ensures that the GUID through the network is verifiable. And the GNRS can collaborate with access control list to fortify security and privacy. The in-network content storage and retrieval at routers ensure that the static content is resistant to flash floods. The block transport combined with storage-aware routing results in better performance to tolerate disruption and realize seamless mobility.

Moreover, the MobilityFirst dynamically binds names with network addresses, which can be anonymous to some extent. Packet forwarding can be constructed in two steps: first by an internetwork routing protocol and then by an intranetwork one. The internetwork routing protocol can be oblivious of the GUID, while the intranetwork one is accomplished with GUID. Hence, only the NA is exposed to the internetwork, which is not fixed and bound with one GUID. This functionality can preserve privacy for consumers and producers, which satisfies the users' requirement for privacy and enhance user acceptance.

2) NetFence: PREVENTING DENIAL OF SERVICE

Besides security embedded in the MobilityFirst, Liu, Yang and Xia proposed NetFence [56] that presents a scalable DoS-resistant network architecture applicable for the MobilityFirst. They designed solutions to suppress attack traffic and resist DoS attacks from the perspective of networks rather than end systems. Each NetFence router holds three channels: request channel with no more than 5% link capacity, regular channel, and legacy channel with low priority.

The NetFence can be used in the MobilityFirst to detect and suppress the DoS attacks to further enhance its security. The NetFence combines prioritization and priority-based rate limitation to ensure the successful transmission of a request by a legitimate sender. The router uses the combination of link load and packet loss rate to indicate a potential attack. Once an attack is detected, a monitoring cycle is started until the attack is ended. At the same time, congestion policing feedback is stamped into the NetFence header of all passing packets, which is policed by an access router. Innocent DoS victims can use the unforgeable congestion policing feedback as a capability token to suppress a bulk of unwanted feedback. Hence, the traffic of DoS damage can be separated from legal traffic.

V. EXPRESSIVE INTERNET ARCHITECTURE (XIA)

As presented above, the NDN and the Coast are content-centric and the MobilityFirst is mobility-centric. Different from these three projects, the XIA [30]–[32] is an Internet architecture project designed with the native support for multiple principals (e.g., hosts, contents, services and networks) and the ability to evolve its functionality to accommodate new principals over time. It is designed with the following goals: be trustworthy, support long-term evolution of usage models, support long-term technology evolution and support explicit interfaces between network actors. This section illustrates the XIA architecture and its security.

A. XIA ARCHITECTURE

The XIA maintains some features of IP protocol, but also introduces several new principles in order to achieve its design goals as described below:

- **Communications between Diverse Principals**: It supports the communications between diverse entities, such as hosts, services, contents and additional principals motivated by future usage models. The different contracts for each principal type enable different communication styles, which can address the evolvability goal of supporting the current and future usage models.
- **Intrinsic Security**: The self-certifying identifiers for all principal types enable principal-specific security. This mechanism allows users to validate an intended counterpart, and check its integrity and accountability.
- **Flexible Addressing**: Flexible addressing supports fallback addressing, which enables a router to deliver a packet even if the router does not support all of destination information that maybe include a newly-introduced principal type. The flexible addressing together with communications between diverse principals can directly support evolvability. It supports client mobility at

the cost of additional indirection through a rebinding mechanism [57].

1) NAMES AND ADDRESSES

As presented above, the XIA supports different principals. The initial XIA defines four basic XIA identifiers (XIDs) as following:

- Host XID (HID): HID is the hash of a host's public key that can be used to validate with whom a principal is interacting. Similar to IP, it can also be used for the purpose of unicasting.
- Service XID (SID): SID deals with the communications with services and realizes anycast, which allows clients to verify the identity of a service. The SID defines what entities do. Note that the SID is different from the service identifier in the MobilityFirst.
- Content XID (CID): CID is defined as the hash of a content, which allows clients to retrieve a desired content from anywhere and check its correctness.
- Network XID (NID): NID specifies a network (i.e., autonomous domain) and allows clients to validate the intended network, with which it is communicating.

The XIA introduces Directed Acyclic Graphs (DAGs) to represent the addresses of XIDs to achieve flexible addressing. The DAGs are highly flexible by allowing packets to express fallbacks and scoping to realize user intent. An example routing technique is given in Fig.1. A "dummy" source "•" represents the conceptual source of a packet and the target is as a sink. Scoping means that the packet must be first routed to a scoping XID before being sent to the destination even if it has the direct route. For example in Fig.1(b), outers deliver the packet to NID first and then forward the packet to an intended SID. Another example of fallback is presented in Fig.1(c). If the SID is not available or recognized, the router will use the fallback NID through a fallback edge (dotted line). Finally, the combined mechanism of scoping and fallback in the DAG is presented in Fig.1(d). Each router along the fallback path can route directly to the intended node.

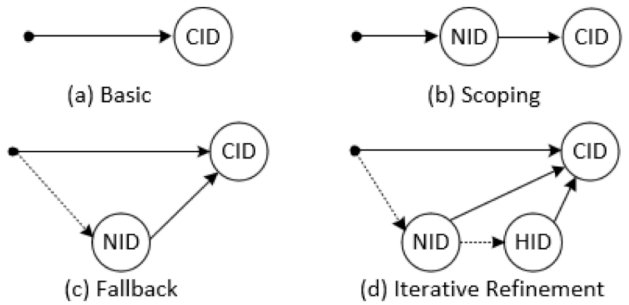

FIGURE 1. Examples of address DAGs.

2) CACHING

Owing to the supporting CID, the XIA enables the opportunistic caching of contents for future services. Similar to the caching in the NDN, routers can also cache the data packets they receive opportunistically. Thus, data consumers can require contents by directly expressing their requests with the CID and retrieve data from either a data producer or content caches of routers. This mechanism can improve the efficiency of data retrieve and save bandwidth. Similar to the caching in the NDN, the CIDs as the cryptographic hash of contents, hold a self-certifying feature and enable any network entities to verify whether the retrieved content matches the identity of the content.

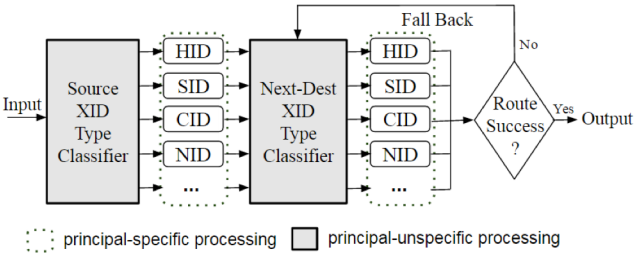

FIGURE 2. XIA forwarding engine of a router.

3) XIA FORWARDING AND ROUTING

The XIA achieves flexible addressing by adopting DAG. An XIA router forwards data packets following the procedure shown in Fig.2. The edge represents the flow of packets. With the development of the XIA, more elements of unknown principals could be added in the dotted boxes. For example, a sourcing content CID_s provided by server HID_s in autonomous domain NID_s would have the DAG: $\cdot \rightarrow \text{NID}_s \rightarrow \text{HID}_s \rightarrow \text{CID}_s$ and a content destination in other domain may have a destination DAG: $\cdot \rightarrow \text{NID}_d \rightarrow \text{HID}_d \rightarrow \text{CID}_d$. First, the packet is passed to a CID processing module by a source classifier based on the XID type of the sink node of the source DAG. Then the router checks the XID of the outbound edges of the last-visited node of the DAG in a priority order. The packet is forwarded along adjacency if the router supports the principal type; If it is not recognized, the packet is returned to the classifier that can check other outbound edges or fallback lines; the destination is unreachable if no outgoing edges work. The forwarding process described above is iteratively executed until it reaches destination CID_d.

B. SECURITY IN XIA NETWORKS

1) INTRINSIC SECURITY

The XIA intrinsically provides secure identifiers. The XID as the hash of public key is associated with a public-private key pair. As stated above, the identifier can be used for checking the integrity of content, validating a counterpart that a principal is communicating with, and ensuring that the content is as expected. Thus, it improves the trustworthiness of end-to-end communications, service access, and content retrieval. Additionally, the XID provides a level of accountability and integrity.

2) PRIVACY

With the rapid development of data mining, privacy has become one of the most important factors to evaluate a new architecture. Fortunately, the XIA research considered the issue of privacy.

As the XIA supports multiple types of identifiers, a device can optionally choose XIDs according to their own use. For example, the device can use one XID for email and another for web search. It is difficult to determine that a same user is involved in multiple activities, which reduces the possibility of tracking.

VI. SCALABILITY, CONTROL, AND ISOLATION ON NEXT GENERATION NETWORK (SCION)

Many patches have been created to fix the vulnerabilities of the current networks due to its lack of security. But it has led to unexpected consequences or the requirement of trust root. Therefore, the SCION [33]–[35], an inter-domain network architecture, was designed to provide route control, failure isolation, and explicit trust information for end-to-end communications. The SCION has the following special features:

- **Availability in Presence of Adversaries**: The architecture is able to circumvent malicious cases such as on-path adversary drops, delays packets, and injects packets into networks, etc.
- **Transparency and Control over Forwarding Paths**: Transparent network path enhances the privacy and security of communications, and path control improves the availability and defends against network attacks by allowing data receivers to select incoming paths.
- **Efficient Trust Management:** The verification of entities is always based on the trust of roots. But it is difficult to enumerate the trust roots as intermediate Certification Authorities (CAs) are always implicitly trusted. Hence, the control over trust root can enable users to easily choose or exclude trust roots regarding to their own willingness. All involved entities globally cannot agree on a single trust root in current PKI models, while a plethora of roots may result in a weakest link of security. Therefore, the SCION designs a global but heterogeneous trust, which is not taken into consideration in other four projects.
- **Efficiency, Scalability, and Extensibility:** Security and high availability usually are achieved at the expense of efficiency and scalability. However, high performance and scalability are of great significance in daily usage, especially economic activities.
- **Foundation for Other Architectures:** P2P communication is the key target due to its advantages in distributed communications.

In what follows, we primarily introduce the architecture of the SCION, and its security issues and countermeasures.

A. SCION ARCHITECTURE

The SCION organizes existing Autonomous Systems (ASes) into groups of independent routing sub-planes called Isolation Domains (ISDs), which are fundamental building blocks in the SCION. Fig.3 gives an example of SCION with three ISDs. Each ISD has one or more ASes acting as an ISD core, and one or more regular ASes. The ISD core negotiates a policy named Trust Root Configuration (TRC) to dominate the ISD, which is described in details in Section 6.1.3. In general, an associated globally-unique human-readable name space is given to each ISD. ASes join an ISD by purchasing a service from one AS in the ISD. The arrow of a link in Fig.3 indicates a provider-customer relationship. All ASes in the ISD should agree on the trust roots and ISD policies operated by some entities. An AS may belong to several ISDs. The use of ISD can provide transparency and support heterogeneous trust environments. In what follows, we present the details of the SCION architecture.

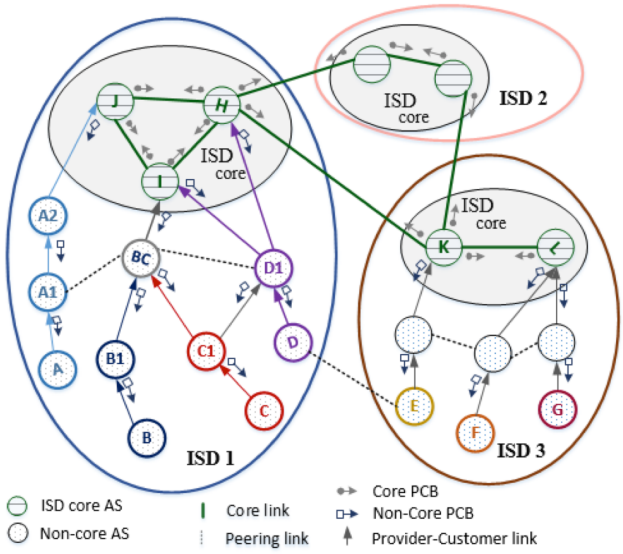

FIGURE 3. Three SCION ISDs with ISD Cores and ASes. The ISD Core ASes are connected via Core links. Non-core ASes are connected via customer-to-provider or peering links.

1) CONTROL PLANE: BEACONING FOR ROUTE DISCOVERY

The SCION supports two levels of routing, named intra-ISD and inter-ISD, which discover routing paths by announcing and distributing Path Construction Beacons (PCBs) within an ISD or among ISD Core ASes. The inter-domain PCB transmission process helps the Core ASes obtain the paths to every other Core AS; while the intra-domain PCB dissemination helps ASes learn the paths to reach the ISD Core ASes.

Fig.4 shows the main components of control plane for discovering paths. As shown in Fig.4(b), each AS consists of three kinds of servers: Beacon Servers for discovering path information by disseminating PCBs, Path Servers for maintaining path segments and disseminating path information, and Certificate Servers for managing key materials and certificates to secure the intra-AS communications. In route

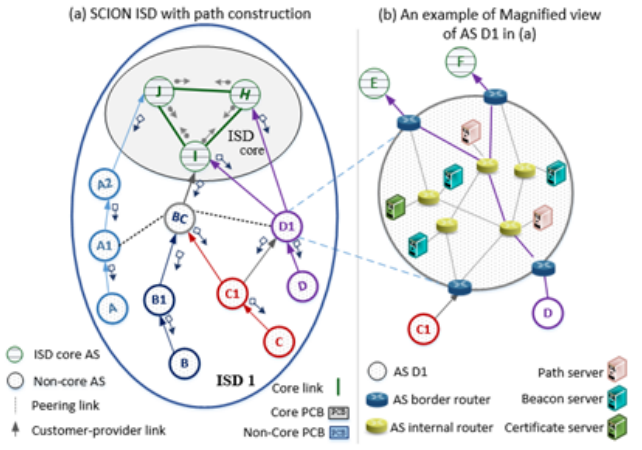

FIGURE 4. **(a) SCION ISD with path construction. (b) Magnified view of AS D1 in (a) with servers and routers.**

discovery, the intra-ISD PCBs in a Core AS will be disseminated to all non-Core ASes in the ISD. Upon receiving the PCBs, the non-Core AS beacon servers resend them to their customer ASes. And each AS adds its interfaces into the PCB. Hence, the PCBs are propagated from the ISD Core to customer ASes, for example, the intra-ISD PCBs transmitted through the path J→A2→A1→A in Fig.4(a). The beaconing process in inter-ISD communications is similar to the route advertising process of Border Gateway Protocol (BGP), except that the process is periodic. After PCB transmission, ASes can choose sets of path segments and upload them to path servers. If a beacon server wants to validate the authenticity of PCBs, it queries a certificate server that keeps the cached copies of TRCs and ASes' certificates.

The SCION end-to-end communication is supported by up to k path segments. Up-segment represents the path segment leads towards an ISD Core; down-segment represents the path segment from the ISD Core to an AS. If a source host wants to communicate with a destination host, it first sends a path resolution request to its local path server that is responsible for forwarding the request to a core path server. The core path server checks if the destination host is within the same ISD as the source host. If yes, the core path server can directly respond the local path server with up to k path segments. Otherwise, the core path server first obtains the corresponding down-segments from a core path server of the destination host. In both cases, the local server returns up to k path segments to the source host. If needed, a core-segment connecting the cores of two ISDs is also provided to the source host.

A SCION path is constructed using the following techniques:

- Immediate path segment combination: If the destination and the source have the same core AS in their path segment, the connection of the up-segment and the down-segment results in a valid end-to-end path. AS B and AS D in Fig.4(a) have the same core AS I, thus their communication path forms as B→B1→BC→I→D1→D.
- AS shortcut: The up-segment and the down-segment intersect at a normal non-Core AS. Then a short path can be obtained by omitting the intersection of the two segments. Though AS B and AS C in Fig.4(a) have the same core AS I, they meet at AS BC and their packets could not be transmitted to core AS I and their path forms an AS shortcut: B→B1→BC→C1→C.
- Peering shortcut: There is a peering link to connect the up-segment and the down-segment and at most one peering link can be used as a shortcut. The extraneous path segment can be omitted to achieve a shortcut relying on the peering link. AS A1 has a peering link with BC in Fig.4(a), thus AS A and AS B can communicate via a peering shortcut path A→A1→BC→B1→B.
- Core-segment combination: The core AS on the up-segment is different from that on the down-segment. For example, a local ISD core-segment (J→I or J→H) is enough for path A→D in Fig.4(a) as they are within the same ISD. But an inter-ISD core-segment (H→K) is required for path A→E in Fig.3 as they belong to different ISDs.

2) DATA PLANE: PACKET CARRIED FORWARDING STATE (PCFS)

As stated above, a control plane takes the charge of providing an end-to-end path, while a data plane is applied to ensure that a packet is indeed forwarded along the path that the control plane offers. A SCION packet contains minimal information. Source and destination are optional as the packet's context is unambiguous without addresses. The SCION router forwards the packet to the next AS based on the AS-level path in the packet header. During the forwarding, a border router verifies if the packet is transmitted through a correct ingress interface and then forwards it to the next hop through a correct egress interface. Only when the packet reaches the destination AS, will the router check the address of destination or packet purpose to forward it to the final destination host.

3) TRUST MANAGEMENT

Traditional certificates, binding identifiers to public keys and carrying digital signatures, are employed to authenticate all entities. However, all parties are difficult to agree on a single trust root in monopoly, while the compromise of a single trusted certification enables forging a server certificate in oligarchy. Therefore, the SCION aims to structure the trust roots while supporting authentication policies.

To achieve flexible trust management, the SCION proposes to allow each ISD to define its own roots of trust and the policy to dominate their usage. The details are presented in [58].

The TRC is in charge of ISDs and defines the roots of trust. A TRC file has a version number that is always updated. Besides the number, it has a list of public keys of trust roots for various purposes and governing policies.

The TRC offers the ability to bootstrap the authentications, achieve trust agility and trust revocation. A user can select an ISD at its own will because the ISDs in the SCION have links among themselves to cross-sign each other's TRC files. Efficient revocation of trust roots can be achieved by following the distribution of PCBs to rapidly disseminate the updated TRC with a new version number.

B. SECURITY IN SCION NETWORKS

To achieve high security, the SCION is equipped with cryptographic mechanisms. First, the trust root of an ISD consists of root key certificates of trusted ISD Core ASes and CAs, and the TRC defines the governing policy, such as which root key certificates are trusted. Second, each AS signs the PCB it forwards, which can be verified by all entities. Furthermore, the application of Packet Carried Forwarding State (PCFS) can ensure the correctness of path. The border routers and beacon servers share one secret key to compute and check Message Authentication Code (MAC) over forwarding information. What's more, the per-AS information including the ingress and egress interfaces, an expiration time and MAC is encoded to be opaque to others, which can protect the privacy of involved communication entities.

In the following subsections, some additional schemes proposed by the SCION team are introduced.

1) SIBRA IN SCION: RESISTING DDoS ATTACKS

The SCION assumes that it has the full control and knowledge of network paths, which lays the foundation of the selection of forwarding path. STRIDE [59] presented a refuge from DDoS attacks based on the SCION, but its construction relies on a non-congestion network, which is difficult to be guaranteed in practice. Then a Scalable Internet Bandwidth Reservation Architecture (SIBRA) [60] was designed to accommodate the SCION architecture for overcoming this problem. The SIBRA uses long-term contracts amongst the Core ASes of large-scale ISDs to establish core paths, intermediate-term contracts amongst ASes within an ISD to establish steady paths, and short-term contracts for end-to-end communications across ISDs to establish ephemeral paths. SIBRA supports the bandwidth reservations and depends on an authenticated reservation token to verify the availability of bandwidth to its neighbors. It can further support statistical multiplexing and bandwidth renewal of an ephemeral path according to a reservation index.

The re-adjustment of bandwidth and the multiplexing between traffic balance the traffic and enable the construction of dynamic inter-domain leased lines. It finally realizes botnet-size independence to defend the DDoS attacks.

2) HORNET: ANONYMITY

Privacy of the Internet users worldwide is at risk and attracts more and more attention. HORNET [61] as a highly-scalable anonymity system was proposed to enhance the privacy with efficiency and payload protection.

Each HORNET node inserts its state into a forwarding packet instead of keeping a per-session state, which is called Forwarding Segment (FS). Then creating nodes can dynamical retrieve the embedded information over an offloading process. During a setup phase, all the FSes are collected depending on a compact and provably secure mix format named Sphinx [62]. In Data Distribution Phase, a source first uses the FSes to construct a forward Anonymous Header (AHDR) and a backward AHDR. The source onion-encrypts its data payloads using shared symmetric session keys, and prepends the AHDR. Each node retrieves its FS, onion-decrypts the packet and forwards it to the next hop until it reaches a destination. Finally, the destination can send the data back to the source using the backward AHDR. Hence, the source that provides the data or service is protected. The anonymity of the source is guaranteed.

The further involvement of a public rendezvous point in the scheme above can realize sender-receiver anonymity, which is omitted for the reason of space limitation. Moreover, the HORNET is not vulnerable to DoS attacks because all states are carried within packets and no per-session memory needs to be stored in nodes or rendezvous points.

3) SOURCE AUTHENTICATION AND PATH VALIDATION

Besides the efforts above, Kim et al. [63] tried to construct higher-level security mechanisms from the perspective of source authentication and path validation. SCION Control Message Protocol (SCMP) is applied in the control plane. In order to efficiently authenticate the SCMP, the SCION gives up the use of digital signature for the possibility of a processing bottleneck when creating lots of SCMP messages. Instead, Kim et al. [63] proposed to enable routers to (re-)create symmetric keys shared with the end hosts on the fly by applying Dynamically Recreatable Key (DRKey) protocol.

In the above scheme, a session is initiated by source node S. In key setup, S first selects a path to destination node D, generates an asymmetric key pair and creates a session identifier. Simultaneously, it prepares some values for authentication and validation. Then an Origin and Path Trace (OPT) packet including these values is forwarded down to destination D. And the router on the path uses it to set up shared symmetric key and then adds some verification field into its header for following verification. During verification, source S precomputes a special authentication field named PVF, which enables D to verify the path using collected path information. The router recreates the shared key based on the PVF to re-compute the verified field and compare it with the data in the packet's header. If the above check passes, it then applies a MAC operation to update the PVF. Repeatedly until it reaches destination D, D finally re-computes fields using all the symmetric keys shared with other entities on the path.

The OPT is similar to the HORNET in dealing with authentication. Both need the source to construct a field for subsequent routing or authentication. Difference is that the HORNET constructs a symmetric key using Diffie-Hellman

key exchange but the OPT uses the DRKey to generate the keys. They both can construct session keys between a destination and intermediate routers.

Through authenticating sources and validating paths, the OPT can construct high-level security mechanisms such as DDoS mitigation, path compliance and packet attribution. This is because that the source authentication guarantees the identity of source and the path validation eliminates the illegal use of path by attackers.

VII. COMPARISON OF FUTURE INTERNET ARCHITECTURES

We have presented five famous future Internet architectures in details: NDN, COAST, MobilityFirst, XIA and SCION. In this section, we present the pros and cons of each and further compare them in terms of a number of security properties: anonymity, authenticity, integrity, privacy, DoS/DDoS resistance, error/fault resilience, and evolvability.

A. PROS AND CONS

As stated above, the NDN and the COAST are content-centric networks. One difference is that the NDN does not validate Interest packets while the COAST verifies all packets. In the NDN, upon receiving an Interest packet at a router, the router will drop the packet or respond with a NACK message if the upper link is down, otherwise it will record the packet in the PIT if the number of PIT entries has not reached its threshold. The cache in the NDN can help reducing workload as it forwards a Data packet to a data consumer as soon as an Interest packet arrives. Naturally, the cache in the NDN also weakens the effect of DDoS attacks through caching. However, it is hard to detect potential attacks without the information about data consumers. Luckily, enhanced security and more functionality can be further offered in the NDN, as described in the work [40], [41], [48], [49]. Some countermeasures to the DDoS attacks were presented in [40] and [41] and privacy problem was researched in [48] and [49]. Contrary to the NDN, the COAST requires all packets including Interest packets to be verified, which can enable the detection of potential DDoS attacks. The COAST with the design of multiple layers can be easily adapted to the current Internet in its architecture and the intelligent nodes in the COAST help filter and check traffic.

Besides the content-centric network architectures, the MobilityFirst is designed to deal with the names and network addresses to achieve mobility, which is actually a hybrid name and address scheme. The MobilityFirst also adopts opportunistic caching to achieve high performance on data delivery.

Baid et al. [64] compared alternative architectures for achieving functional goals of name oriented networking, mainly the NDN and the MobilityFirst. Each router needs to maintain a unique or an aggregated entry in its routing table for each name. The routing table needs to scale to the total number of named objects, which leads to specific issues with scalability. The MobilityFirst tries to solve the problem by decoupling the routing table from the content space size and dividing the problem into two distinct parts: 1) mapping by the GNRS; 2) routing protocol for distributing a routing table. Compared with the NDN, the MobilityFirst has a smaller routing table size. In addition, it has a lower updating overhead because the content changes would not affect the network routing layer. But the changes would seriously affect the name-based routing protocol.

Li et al. [65] further explored two architectures based on the NDN and the MobilityFirst respectively to support Internet of Things (IoT) and compared them through simulations. The results show that the MobilityFirst has lower control overheads with comparable performance in delay, throughput and packet success rate.

In contrast to the three projects (NDN, COAST and MobilityFirst), the XIA has the advantage of supporting diverse entities, including content principals, service principals, network principals and even unknown future principals. Another outstanding feature is that it supports the fallback mechanism to offer scalability and evolvability. Furthermore, the integration of the SCION with the XIA achieves a higher security than the above three architectures, including accountability, anonymity and availability. In order to maintain trust relationships, each entity should hold a secure identifier besides the changeable and various XIDs. Otherwise, an adversary can register into the network with a new identifier that may eliminate its ever-bad records, which results in inaccurate trust evaluation.

With greater efforts on security research, the SCION presents more security properties than other four projects, e.g., resisting DDoS attacks, anonymity, authentication, etc. Trust management is mentioned in the NDN, the COAST, and the MobilityFirst as a key technical challenge. But none of them gives a concrete method to manage trust. The SCION presents a detailed discussion on trust management. It adopts the notions of ISDs and TRC to control trust efficiently, which can dominate its own trust and limit the influence of compromised trust root within its own ISD.

We summarize the high-level overall pros and cons of each project in Table 1.

B. COMPARISON

By analyzing the five projects, we can find that eight security properties are concerned: confidentiality, anonymity, authenticity, integrity, privacy, DDoS resistance, evolvability and (error and fault) resilience to the presence of adversaries. In order to get a holistic knowledge of the security requirements and countermeasures, we further compare the five projects from the eight security properties and summarize the results in Table 2. Some security features are innate in the network architecture design, while some are reinforced by additional research efforts.

Data confidentiality is one vital component of data security, which prevents unauthorized access to data. If end-to-end communication can be built, confidentiality can be easily guaranteed through cryptographic mechanisms

TABLE 1. Pros and Cons of the five projects.

Projects	Pros	Cons
NDN	Low networking workload with caching; Verification of Data packets; Self-regulating traffic to achieve flow balance.	Unclear organization and management of name space; Large routing table size to accommodate the huge number of named objectives; Lack of access control; High update overhead.
COAST	Intelligence on traffic check and filtering; Verification of all packets; Detection of attacks.	Large routing table size to accommodate a huge number of named objectives; High update overhead; Lack of access control; Too much processing at network nodes.
MobilityFirst	Separation of names and network addresses for supporting high mobility; Seamless mobility; Self-certifying GUID for authentication.	Difficult for global resolution; Difficult to obtain tradeoff on scalability and mobility; Difficult to guarantee secure communications when endpoints have different NCSes.
XIA	Supporting diverse principals; Flexible addressing; Cryptographically generated identifiers for offering innate security.	Large overhead: 160-bit XID in the XIA packet header; Complex trust and principal management.
SCION	Novel trust models; Confining attacks into separated isolation domains; High flexibility with separation of control plane and data plane.	Lack of the integration of all security designs into the architecture; Unclear how to seamlessly integrate the SCION with other proposals.

TABLE 2. Comparison of the five projects regarding security properties.

Project Names / Properties	NDN	COAST	MobilityFirst	XIA	SCION
Confidentiality	Lower	Lower	Higher	Higher	Higher
Anonymity	Higher	Higher	Medium	Lower	Higher
Authenticity	√	√	√	√	√
Data Integrity	√	√	√	√	--
Privacy	Medium	Medium	Higher	Lower	Higher
DoS/DDoS Resistance	Lower	Medium	Higher	Higher	Higher
Resilience	Lower	Medium	Medium	--	Higher
Evolvability	--	√	√	√	--

Notes: --: not applicable or not mentioned; √: satisfied; other descriptions represent security level achieved for each security property.

(e.g., symmetric encryption). As stated above, the XIA, the MobilityFirst and the SCION can easily construct end-to-end communications, while the NDN and the COAST cannot. Moreover, the cached data in the NDN and the COAST are available to all users, thus it is difficult to deploy access control mechanism and achieve confidentiality. Though HONS [52] and access control policy provide partial confidentiality, confidentiality is still a crucial problem.

The HORNET [61] and the ANDaNA [46] were designed to enhance the anonymity of the SCION and the NDN respectively. The MobilityFirst can achieve partial anonymity based on dynamical binding. The COAST entity can also be anonymous using the HONS.

The HONS enables content-centric architectures (the NDN and the COAST) to achieve data authentication. The signature used in the NDN further provides non-repudiation in addition to authentication. In addition, Yu et al. [66] designed a model for the NDN to authenticate long-lived data in case of failure caused by the short validity period of certification. The hash of content or public key is used in the MobilityFirst and the XIA to achieve both authentication and data integrity. The SCION's accountability can be enhanced by using the OPT [63].

Privacy is a key problem nowadays. All these projects have paid attention to it. Particularly, an attacker may be able to infer privacy information by observing the speed of data

responses in the NDN and the COAST, especially for highly sensitive contents. Though such inference can be overcome in a certain degree by delaying data delivery, it causes some impact on network performance. Privacy protection in the XIA can be achieved by choosing different XIDs for different purposes, which somewhat can prevent tracking but may not be sufficient in many applications. The dynamic bindings of names and network addresses in the MobilityFirst and the HORNET can achieve higher privacy protection.

The data centric nature of the NDN makes it vulnerable to some special DDoS attacks, such as Interest flooding and content poisoning, hence some countermeasures [40], [41] were proposed. The content filtering and qualification process in the COAST are able to mitigate DDoS attacks but no detailed discussions were given in the literature. Intrinsic security in the MobilityFirst and the XIA allows the network to validate the sources of contents that is certainly useful to mitigate DDoS attacks. The NetFence [56] for the MobilityFirst and the SIBRA [60] for the SCION were designed to resist DDoS attacks.

The incremental deployment of intelligent services and virtual overlays in the COAST make it evolvable. The computing and storage layer in the MobilityFirst and the introduction of new principals in the XIA can both support evolvability.

The packet retransmission supported by caching ensures the resilience of the NDN in a passive way. The COAST obtains a good resilience to node failures at the cost of overhead to have good knowledge of network segments. Trustworthiness and verifiable identifier in the MobilityFirst reinforce the network resilience in the presence of certain malicious adversaries: Multi-path communications in the SCION make it fault and attack resilient.

The above comparisons are based on the design documents and silent features of the five future Internet architectures, which are not sufficient to conclude which architectures are superior. This is true since all the projects are at an early stage and lack sufficiently large scale testing and deployment. However, our comparisons indeed provide a high level understanding of theses architectures. Based on these comparisons, we present a number of important security issues that need to be addressed in future research in the next section.

VIII. DISCUSSIONS AND PERSPECTIVES

Having presented an overview and comparison of the five future Internet architectures, we further give a perspective of the security problems and some potential countermeasures. We also provide a list of security issues worth further study in the future.

A. SECURITY ISSUES

From the discussions above, we can see that several security issues have been taken into consideration by all projects and should be embedded in the network designs towards building a holistic future Internet architecture:

1) DATA CONFIDENTIALITY

Data over the network are easily accessed by adversaries and unauthorized consumers. Confidentiality should be guaranteed to prevent eavesdropping.

Confidentiality can be achieved through cryptography (e.g., symmetric encryption, asymmetric encryption, PRE). Besides the traditional mechanism, q-RPB scheme introduced in HONS and access control policy (e.g., publish/subscribe scheme) are two other ways to achieve the data confidentiality, especially for content-centric networks.

2) DATA INTEGRITY

Data are transmitted through the network and exposed to many adversaries. They are subjected to injection and manipulation during transmission. In order to obtain the correct and complete data, the integrity of data is one of the most important issues for content-centric networks.

Towards this goal, two main approaches have been proposed. One is the digital signature used in the NDN. Each data packet is signed to support integrity check. Another approach is to apply the hash value of content as self-certifying identifier in the MobilityFirst and the XIA, which results in the same effect but could be more efficient.

3) AUTHENTICITY

To resist impersonation attacks, authentication has been considered in all these projects using the same techniques as data integrity. In addition, routers in the OPT [63] compute and update the authentication field in a packet one by one, which enables the destination to authenticate the source and even the routing path.

4) DoS/DDoS RESISTANCE

Though routers and other intelligent networking devices in the future Internet are much more powerful than their counterparts in today's Internet, they are still vulnerable to DoS/DDoS attacks, which can trigger a massive number of compromised machines or zombies to exhaust vast but still limited resources. Resistance to the DoS/DDoS attacks has been a priority in all the five projects.

Three approaches have been proposed in the five projects to mitigate the DoS/DDoS attacks. Caching is one of the simplest approaches, which can circumvent the redistribution of the same content requests and save bandwidth, though it brings some negative effects (for example, privacy issue) that need to be addressed [67]–[69]. Intrinsic security also contributes positively towards mitigation of the DoS/DDoS attacks since it ensures the transmission of legal traffic. Perhaps the most effective approach is bandwidth management during routing path establishment such as the SIBRA [60] and the congestion policing feedback as proposed in the NetFence [56]. They both cope with the DoS/DDoS problem from the perspective of guaranteed bandwidth. That is, they guarantee the successful delivery of legitimate requests and data by reserving the bandwidth for authorized users ahead of time.

5) SENDER/RECEIVER ANONYMITY

In some sensitive scenarios, it is necessary to conceal the addresses of destinations and sources. Today's Internet offers weak privacy protection. One can find out who are the sender and the recipient by checking the source and destination addresses. Obviously, separation of identifiers and addresses is the most efficient way for enhancing sender/receiver anonymity. Content-centric networks even do not involve the addresses of the source and destination and just specify data names. The MobilityFirst separates the human readable name from the network address and dynamically binds them for communications. The HORNET [61] achieves this goal with anonymous header and onion-encryption, which provides stronger anonymity but with the cost of higher overhead due to the additional encryption and decryption operations.

6) USER PRIVACY

With the pervasiveness of communications, data mining and cloud computing, user privacy becomes increasingly a serious concern, which even influences the user acceptance of many networking services. Except for anonymity, anti-inference is another crucial issue with regard to user privacy. Since content caching is used in all of the five projects, network neighbors may learn about each other's content accesses using timing information to identify cache hits. A method proposed in the NDN to address this problem is to introduce delays in data delivery. But this solution could impact networking performance.

7) RESILIENCE

In terms of resilience to network errors/faults and malicious attacks, the passive way of retransmission after failure is one effective method. Besides, domain isolation based on trustworthiness in the SCION would be a good solution to confine the damage of attacks to a single domain.

8) EVOLVABILITY

From the lessons of today's Internet, evolvability must be supported in the design of the future Internet. It is impossible to forecast what will come in the future and encapsulate all of them into the design now. Evolvability can satisfy the requirements and guarantee its continuous suitability.

The COAST supports evolvability through deployment of intelligent services, a new layer or principal can be adopted to solve this issue. The XIA supports evolvability by accommodating multiple principal types, including unknown types in the future.

B. FUTURE SECURITY RESEARCH ISSUES

All of the five future Internet projects put security as high priority in their designs. However, all the projects, except the SCION, only provided a very coarse description on the core security techniques and the desirable security features without in-depth investigation, thus left many open issues. The following is a list of open security issues that we believe are important for achieving the security goals of the future Internet and hence need to be studied carefully in the future.

1) ACCESS CONTROL

Traditional countermeasures are not very suitable for ICN due to the absence of hosts and the adoption of caching. Hence, a flexible and practical access control mechanism is needed to realize data confidentiality.

- How to control the access to data cached widely at routers? Attribute-Based Encryption (ABE) [70], [71] can be potentially applied to solve this problem. The control policies can be regarded as attributes to protect data.
- Trust can be introduced to judge access. It can be used to evaluate data consumers or routers, and thus impel involved routers to behave honestly. The combination of trust and ABE would be another direction, such as the work described in [72].

2) EFFICIENT SIGNATURES

Signature plays a vital role in all five future Internet architectures. All Data packets in the NDN are signed and ASes in the SCION signs all routing requests (e.g., PCBs). Hence, they all call for a more efficient signature algorithm than normal ones to adapt to newly designed network.

- To realize high speed networking, signature generation and verification must be extremely efficient. There is also an urgent need to study and standardize efficient post-quantum computer digital signature schemes.

3) DATA ORGANIZATION AND NAME MANAGEMENT

Due to the lack of host in the NDN and the COAST, names are widely used to represent the content and work as IP address. The NDN router needs to cache data entries. In the COAST, the binding relationship between contents and names should be stored. In the XIA, names are derived from hashing data. However, the following issues need to be systematically studied:

- How to name data with complicated structures (e.g., scalable multimedia data)?
- How to deal with bit errors and packet losses while allowing verifiability if the name is derived from hashing of the data? Some studies [73]–[76] have been done in multimedia authentication, which may offer some guidelines to solve this problem.
- How to name data generated in real-time?
- Routers or network intelligent devices hold large routing tables for named objects. How to organize them to achieve fast delivery while resisting DDoS attacks?

4) AVAILABILITY AND DDoS RESISTANCE

Today's Internet supports many critical applications that underpin the foundations of our modern society. However, the current state of availability of the Internet is far from being commensurate given its importance. Numerous efforts

are required to study availability issues in the future Internet, and in particular, techniques to detect and mitigate DDoS attacks.

- How to detect and prevent attacks by legitimate entities that are able to produce verifiable network requests and data?
- How to detect and prevent cache poisoning attacks in content-centric networks?

5) SCALABLE AND FLEXIBLE TRUST MANAGEMENT

The paradigms of monopoly and oligarchy in trust management have their own pros and cons. Entities widely distributed are difficult to agree on one trust root. The SCION proposed to depend on isolation domains to manage trust roots. But how to formulate trust criteria and evaluate trust is also an open problem. The other projects, i.e., NDN, MobilityFirst, COAST and XIA, simply assume the existence of a scalable and flexible trust management structure without providing any detailed discussions. A number of additional issues as listed below should be seriously studied before deploying the proposed architecture in practice.

- How to agree on roots of trust and maintain their resilience at the Internet scale?
- How to manage, store, and revoke certificates for billions of devices, including end user devices, network nodes and services? The XIA and the MobilityFirst are designed for intrinsic security. That is, network entities can validate integrity and authenticity without checking with external databases (i.e., a certificate revocation database). Then how to verify that a certificate or identity has not been revoked?
- Network identifiers derived from the hash of public keys are not hierarchical. Similarly, data names derived from the hash of data content are not hierarchical. Yet hierarchical names and identifiers are essential for efficient routing. A possible approach to solve the problem is exploring hierarchical identity-based encryption and signature schemes that allows distributed key generation and management. Again, key revocation is an extremely challenging issue.

6) TRADEOFF ON MOBILITY AND SCALABILITY

In the MobilityFirst, core-edge routing supports a two-level hierarchy. A core router and an edge router hold different forwarding entries, which can reduce the number of forwarding table entries stored in the routers. But it limits the mobility. Other projects provide certain supports on mobility by rebinding or re-transmission, but how to arrive at a fair tradeoff on scalability and mobility is still an open issue.

7) A UNIFIED AND HOLISTIC SECURITY ARCHITECTURE

Every project has its own pros and cons and focuses on different aspects of security. It is a crucial task to construct a unified and holistic security architecture for the future Internet.

IX. CONCLUSION

The Internet was designed some 40 years ago and has been successful beyond even the most optimistic expectations. However, it is facing many challenges, including scalability, mobility, availability and security. The diverse services especially economic activities and the dominant use of the Internet as distributed networks call for a clean slate design of new Internet architecture, which embeds security as an intrinsic feature. So far, many research efforts have been carried out all over the world on the research of the Future Internet. In this survey, we looked at five of these projects: NDN, COAST, MobilityFirst, XIA and SCION. We presented their motivations and architecture designs, analyzed their security goals and techniques and provided a comparison of the five architectures. Finally, we mentioned the main security issues that must be kept in mind during the Internet architecture design and proposed a number of open issues for future research.

REFERENCES

[1] B. M. Leiner *et al.*, "A brief history of the Internet," *ACM SIGMOBILE Comput. Commun. Rev.*, vol. 39, no. 5, pp. 22–31, 2009.
[2] J. Postel, *Internet Protocol*, document RFC 791, 1981.
[3] S. Deering and R. Hinden, *Internet Protocol, Version 6 (IPV6) Specification*, document RFC 2460, 1998.
[4] *New Zealand IPv6 Task Force. FAQs*, accessed on May 20, 2016. [Online]. Available: http://www.ipv6.org.nz/ipv6-faqs/
[5] M. Leber. *Global IPv6 Deployment Progress Report*, accessed on Jun. 26, 2016. [Online]. Available: http://bgp.he.net/ipv6-progress-report.cgi
[6] Google. *IPv6*, accessed on Jun. 12, 2016. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption
[7] *IPv4 Address Report*, accessed on Jun. 26, 2016. [Online]. Available: http://www.potaroo.net/tools/ipv4/
[8] B. Sinclair. (Nov. 4, 2013). *Biggest Risks in IPv6 Security Today*. [Online]. Available: http://www.networkworld.com/article/2171504/tech-primers/biggest-risks-in-ipv6-security-today.html
[9] B. Daya, "Network security: History, importance, and future," Dept. Elect. Comput. Eng., Univ. Florida, Gainesville, FL, USA, 2013.
[10] S. Kent and K. Seo, *Security Architecture for the Internet Protocol*, document RFC 4301, 2005.
[11] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, *DNS Security Introduction and Requirements*, document RFC 4033, 2005.
[12] P. Stuckmann and R. Zimmermann, "European research on future Internet design," *IEEE Wireless Commun.*, vol. 16, no. 5, pp. 14–22, Oct. 2009.
[13] European Community Future Internet Architecture (FIArch) Experts Group. (Mar. 2011). *Fundamental Limitations of Current Internet and the Path to Future Internet*. [Online]. Available: http://www.umic.pt/images/stories/publicacoes4/fiarch-current-internet-limitations-march2011.pdf
[14] M. Handley, "Why the Internet only just works," *BT Technol. J.*, vol. 24, no. 3, pp. 119–129, 2006.
[15] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Commun. Mag.*, vol. 50, no. 7, pp. 26–36, Jul. 2012.
[16] J. Pan, S. Paul, and R. Jain, "A survey of the research on future Internet architectures," *IEEE Commun. Mag.*, vol. 49, no. 7, pp. 26–36, Jul. 2011.
[17] G. Xylomenos *et al.*, "A survey of information-centric networking research," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1024–1049, May 2014.
[18] L. Zhang *et al.*, "Named data networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, 2014.
[19] L. Zhang *et al.*, "Named data networking (NDN) project," Palo Alto Res. Center, Palo Alto, CA, USA, Tech. Rep. 2010-003, 2010.
[20] *Named Data Networking*, accessed on Oct. 20, 2015. [Online]. Available: http://named-data.net/

[21] *NSF Future Internet Architecture Project*, accessed on Oct. 25, 2015. [Online]. Available: http://www.nets-fia.net/
[22] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in *Proc. 5th Int. Conf. Emerg. Netw. Exp. Technol. (CoNEXT)*, Rome, Italy, 2009, pp. 1–12.
[23] *COAST: Content Aware Searching Retrieval and sTreaming*, accessed on Nov. 9, 2015. [Online]. Available: http://www.synelixis.com/coast/
[24] T. Zahariadis, F. Junqueira, L. Celetto, E. Quacchio, S. Niccolini, and P. Plaza, "Content aware searching, caching and streaming," in *Proc. 2nd Int. Conf. Telecommun. Multimedia*, Chania, Greece, 2010, pp. 263–265.
[25] (Jun. 15, 2016). *FP7 Projects*. [Online]. Available: http://www.future-internet.eu/activities/fp7-projects.html
[26] D. Raychaudhuri, K. Nagaraja, and A. Venkataramani, "MobilityFirst: A robust and trustworthy mobility-centric architecture for the future Internet," *ACM SIGMOBILE Comput. Commun. Rev.*, vol. 16, no. 3, pp. 2–13, 2012.
[27] I. Seskar, K. Nagaraja, S. Nelson, and D. Raychaudhuri, "MobilityFirst future Internet architecture project," in *Proc. 7th Asian Int. Eng. Conf. (AINTEC)*, Bangkok, Thailand, 2011, pp. 1–3.
[28] A. Venkataramani, J. Kurose, D. Raychaudhuri, K. Nagaraja, M. Mao, and S. Banerjee, "MobilityFirst: A mobility-centric and trustworthy Internet architecture," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 74–80, 2014.
[29] *MobilityFirst Future Internet Architecture Project Overview*, accessed on Nov. 15, 2015. [Online]. Available: http://mobilityfirst.winlab.rutgers.edu/
[30] D. Han *et al.*, "XIA: Efficient support for evolvable internetworking," in *Proc. NSDI*, 2012, pp. 309–322.
[31] D. Naylor *et al.*, "XIA: Architecting a more trustworthy and evolvable Internet," *ACM SIGMOBILE Comput. Commun. Rev.*, vol. 44, no. 3, pp. 50–57, 2014.
[32] *eXpressive Internet Architecture*, accessed on Nov. 25, 2015. [Online]. Available: https://www.cs.cmu.edu/~xia/
[33] D. Barrera, R. M. Reischuk, P. Szalachowski, and A. Perrig. (2015). "SCION five years later: Revisiting scalability, control, and isolation on next-generation networks." [Online]. Available: http://arxiv.org/abs/1508.01651
[34] X. Zhang, H.-C. Hsiao, G. Hasker, H. W. Chan, A. Perrig, and D. G. Andersen, "SCION: Scalability, control, and isolation on next-generation networks," in *Proc. IEEE Secur. Privacy (SP)*, Berkeley, CA, USA, May 2011, pp. 212–227.
[35] *SCION: Scalability, Control, and Isolation on Next-Generation Networks*, accessed on Dec. 5, 2015. [Online]. Available: http://www.scion-architecture.net/
[36] D. Smetters and V. Jacobson, "Securing network content," PARC, Palo Alto, CA, USA, Tech. Rep. TR-2009-01, Oct. 2009.
[37] H. Yuan and P. Crowley, "Reliably scalable name prefix lookup," in *Proc. 11st ACM/IEEE Symp. Archit. Netw. Commun. Syst. (ANCS)*, Oakland, CA, USA, 2015, pp. 111–121.
[38] H. Yuan, T. Song, and P. Crowley, "Scalable NDN forwarding: Concepts, issues and principles," in *Proc. 21st Int. Conf. Comput. Commun. Netw. (ICCCN)*, Munich, Germany, 2012, pp. 1–9.
[39] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker, "Naming in content-oriented architectures," in *Proc. ACM SIGCOMM Workshop Inf.-Centric Netw. (ICN)*, Toronto, ON, Canada, 2011, pp. 1–6.
[40] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "Dos and DDoS in named data networking," in *Proc. 22nd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Nassau, Bahamas, 2013, pp. 1–7.
[41] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: Mitigating interest flooding DDoS attacks in named data networking," in *Proc. IEEE 38th Conf. Local Comput. Netw. (LCN)*, Sydney, NSW, Australia, 2013, pp. 630–638.
[42] S. DiBenedetto and C. Papadopoulos. (2015). *Mitigating Poisoned Content With Forwarding Strategy*. [Online]. Available: http://www.cs.colostate.edu/TechReports/Reports/2015/tr15-101.pdf
[43] Y. Yu, A. Afanasyev, D. Clark, V. Jacobson, K. Claffy, and L. Zhang, "Schematizing trust in named data networking," in *Proc. 2nd Int. Conf. Inf. Centric Netw. (ICN)*, San Francisco, CA, USA, 2015, pp. 177–186.
[44] A. Broder and M. Mitzenmacher, "Network applications of bloom filters: A survey," *Internet Math.*, vol. 1, no. 4, pp. 485–509, 2004.
[45] W. L. Fu, H. B. Abraham, and P. Crowley, "Synchronizing namespaces with invertible bloom filters," in *Proc. 11th ACM/IEEE Archit. Netw. Commun. Syst. (ANCS)*, Oakland, CA, USA, May 2015, pp. 123–134.
[46] S. DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun. (2011). "ANDaNA: Anonymous named data networking application." [Online]. Available: https://arxiv.org/abs/1112.2205
[47] A. Anand, A. Gupta, A. Akella, S. Seshan, and S. Shenker, "Packet caches on routers: The implications of universal redundant traffic elimination," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 4, pp. 219–230, 2008.
[48] G. Acs, M. Conti, P. Gasti, C. Ghali, and G. Tsudik, "Cache privacy in named-data networking," in *Proc. IEEE 33rd Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Philadelphia, PA, USA, Jul. 2013, pp. 41–51.
[49] A. Chaabane, E. D. Cristofaro, M. A. Kaafar, and E. Uzun, "Privacy in content-oriented networking: Threats and countermeasures," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 3, pp. 25–33, Jul.2013.
[50] N. Fotiou, G. F. Marias, and G. C. Polyzos, "Towards a secure rendezvous network for future publish/subscribe architectures," in *Proc. Future Internet Symp. (FIS)*, 2010, pp. 49–56.
[51] N. Fotiou, G. F. Marias, and G. C. Polyzos, "Access control enforcement delegation for information-centric networking architectures," in *Proc. 2nd ICN Workshop Inf. Centric Netw.*, Helsinki, Finland, 2012, pp. 85–90.
[52] J. Jeong, T. T. Kwon, and Y. Choi, "Host-oblivious security for content-based networks," in *Proc. 5th Int. Conf. Future Internet Technol.*, Seoul, South Korea, 2010, pp. 35–40.
[53] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Secur. Privacy (SP)*, Oakland, CA, USA, May 2003, pp. 197–213.
[54] "The next-phase MobilityFirst project—From architecture and protocol design to advanced services and trial deployments," Project. Rep., 2016. [Online]. Available: http://mobilityfirst.winlab.rutgers.edu/documents/MF_FIA_NP_Annual_Report_final_2016R.pdf
[55] S. C. Nelson, G. Bhanage, and D. Raychaudhuri, "GSTAR: Generalized storage-aware routing for MobilityFirst in the future mobile Internet," in *Proc. 6th Int. Workshop MobiArch*, Bethesda, MD, USA, 2011, pp. 19–24.
[56] X. Liu, X. W. Yang, and Y. Xia, "NetFence: Preventing Internet denial of service from inside out," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, pp. 255–266, Oct. 2011.
[57] A. C. Snoeren and H. Balakrishnan, "An end-to-end approach to host mobility," in *Proc. 6th Int. Conf. Mobile Comput., Netw.*, Boston, MA, USA, 2000, pp. 155–166.
[58] S. Matsumoto, R. M. Reischuk, P. Szalachowski, T. H.-J. Kim, and A. Perrig. (2015). "Designing a global authentication infrastructure." [Online]. Available: http://arxiv.org/abs/1506.03392
[59] H.-C. Hsiao *et al.*, "STRIDE: Sanctuary trail–refuge from Internet DDoS entrapment," in *Proc. 8th ACM SIGSAC Inf. Comput. Commun. Secur. (AsiaCCS)*, Hangzhou, China, 2013, pp. 415–426.
[60] C. Basescu *et al.* (2015). "SIBRA: Scalable Internet bandwidth reservation architecture." [Online]. Available: https://arxiv.org/abs/1510.02696
[61] C. Chen, D. E. Asoni, D. Barrera, G. Danezis, and A. Perrig, "HORNET: High-speed onion routing at the network layer," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, Denver, CO, USA, 2015, pp. 1441–1454.
[62] G. Danezis and I. Goldberg, "Sphinx: A compact and provably secure mix format," in *Proc. 30th IEEE Secur. Privacy (SP)*, Berkeley, CA, USA, May 2009, pp. 269–282.
[63] T. H.-J. Kim, C. Basescu, L. Jia, S. B. Lee, Y.-C. Hu, and A. Perrig, "Lightweight source authentication and path validation," in *Proc. ACM Conf. SIGCOMM*, Chicago, IL, USA, 2014, pp. 271–282.
[64] A. Baid, T. Vu, and D. Raychaudhuri, "Comparing alternative approaches for networking of named objects in the future Internet," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Orlando, FL, USA, Mar. 2012, pp. 298–303.
[65] S. Li, Y. Zhang, D. Raychaudhuri, and R. Ravindran, "A comparative study of MobilityFirst and NDN based ICN-IoT architectures," in *Proc. 10th Int. Conf. Heterogen. Netw. Qual., Rel., Secur. Robustness (QShine)*, Rhodes, Greece, Aug. 2014, pp. 158–163.
[66] Y. D. Yu, A. Afanasyev, and L. Zhang, "NDN DeLorean: An authentication system for data archives in named data networking," NDN, San Diego, CA, USA, Tech. Rep. NDN-0040, May 2016.
[67] W. K. Chai, D. L. He, I. Psaras, and G. Pavlou, "Cache 'less for more' in information-centric networks," in *Proc. 11th Int. IFIP TC Netw. Conf.*, 2012, pp. 27–40.
[68] I. Psaras, W. K. Chai, and G. Pavlou, "Probabilistic in-network caching for information-centric networks," in *Proc. 2nd ed. ICN Workshop Inf. Centric Netw.*, Helsinki, Finland, 2012, pp. 55–60.

[69] G. Carofiglio, V. Gehlen, and D. Perino, "Experimental evaluation of memory management in content-centric networking," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–6.
[70] S. Luo, J. Hu, and Z. Chen, "Ciphertext policy attribute-based proxy re-encryption," in *Information and Communications Security*, vol. 6476. Springer, 2010, pp. 401–415.
[71] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS)*, Alexandria, VA, USA, 2006, pp. 89–98.
[72] Z. Yan, X. Y. Li, M. J. Wang, and A. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Trans. Cloud Comput.*, vol. PP, no. 99, p. 1, 2015.
[73] R. H. Deng, X. Ding, and S. W. Lo, "Efficient authentication and access control of scalable multimedia streams over packet–lossy networks," *Secur. Commun. Netw.*, vol. 7, no. 3, pp. 611–625, Mar. 2014.
[74] A. Habib, D. Xu, M. Atallah, B. Bhargava, and J. Chuang, "A tree-based forward digest protocol to verify data integrity in distributed media streaming," *IEEE Trans. Knowl. Data Eng.*, vol. 17, no. 7, pp. 1010–1014, Jul. 2005.
[75] M. Hefeeda and K. Mokhtarian, "Authentication schemes for multimedia streams: Quantitative analysis and comparison," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 6, no. 1, pp. 1–24, Feb. 2010.
[76] J. M. Park, E. K. P. Chong, and H. J. Siegel, "Efficient multicast stream authentication using erasure codes," *ACM Trans. Inf. Syst. Secur.*, vol. 6, no. 2, pp. 258–285, May 2003.

WENXIU DING received the B.Eng. degree in information security from Xidian University, Xi'an, China, in 2012, where she is currently pursuing the Ph.D. degree in information security from the School of Telecommunications Engineering. She was a Visiting Research Student with the School of Information Systems, Singapore Management University. Her research interests include RFID authentication, privacy preservation, data mining, and trust management.

ZHENG YAN (M'06–SM'14) received the B.Eng. degree in electrical engineering and the M.Eng. degree in computer science and engineering from Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, the M.Eng. degree in information security from the National University of Singapore, Singapore, in 2000, and the Licentiate degree of Science and the D.Sc. degree in technology in electrical engineering from the Helsinki University of Technology, Helsinki, Finland, in 2005 and 2007, respectively. She is currently a Professor with the Xidian University, Xi'an, and a Visiting Professor with the Aalto University, Espoo, Finland. She has authored over 140 publications and solely authored two books. She is the inventor and co-inventor of 46 patents and patent applications. Her research interests are in trust, security and privacy, social networking, cloud computing, networking systems, and data mining. She serves as an Editor/Guest Editor and an Organization and Program Committee Member for numerous international journals, conferences, and workshops.

ROBERT H. DENG (F'16) is a Professor at the School of Information Systems, Singapore Management University since 2004. His research interests include data security and privacy, multimedia security, network and system security. He has served/is serving on the editorial boards of many international journals in security, such as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, and the International Journal of Information Security. He is the chair of the Steering Committee of the ACM Asia Conference on Computer and Communications Security (ASIACCS). He received the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006. He was named Community Service Star and Showcased Senior Information Security Professional by $(ISC)^2$ under its Asia-Pacific Information Security Leadership Achievements program in 2010.