A Survey of Security Attacks in Information-Centric Networking

Eslam G. AbdAllah, *Student Member, IEEE*, Hossam S. Hassanein, *Senior Member, IEEE*, and Mohammad Zulkernine, *Senior Member, IEEE*

***Abstract*—Information-centric networking (ICN) is a new communication paradigm that focuses on content retrieval from a network regardless of the storage location or physical representation of this content. In ICN, securing the content itself is much more important than securing the infrastructure or the endpoints. To achieve the security goals in this new paradigm, it is crucial to have a comprehensive understanding of ICN attacks, their classification, and proposed solutions. In this paper, we provide a survey of attacks unique to ICN architectures and other generic attacks that have an impact on ICN. It also provides a taxonomy of these attacks in ICN, which are classified into four main categories, i.e., naming, routing, caching, and other miscellaneous related attacks. Furthermore, this paper shows the relation between ICN attacks and unique ICN attributes, and that between ICN attacks and security requirements, i.e., confidentiality, integrity, availability, and privacy. Finally, this paper presents the severity levels of ICN attacks and discusses the existing ICN security solutions.**

***Index Terms*—Information-centric networking (ICN), taxonomy of ICN attacks, ICN security, severity levels of ICN attacks.**

I. Introduction

According to Cisco Visual Networking Index 2013, global IP traffic per month will reach approximately 126 Exabytes and the sum of all forms of video will be between the range of 80 to 90 percent of global consumer traffic by the year 2017 [1]. These new requirements of increasing demand for highly scalable and efficient distribution of content require new alternative solutions for the upcoming Internet era, as the existing Internet architecture is becoming inadequate [2]. Information-centric networking (ICN) is one of these alternatives [3]. ICN architectures focus on contents or information objects and their properties in the network. ICN is also concerned about receiver interests. In order to achieve these goals, ICN relies on location independent naming, in-network caching, and name-based routing.

In ICN, senders do not send content directly to receivers. A sender publishes advertisement messages to tell the network that it has some content to share, without necessarily knowing who may be interested in it. On the other side, a receiver declares its interest for some content, not necessarily knowing the senders who have published this content. The ICN network makes a delivery path from the sender to the receiver when there is a match between sender's publication and receiver's subscription. Finally, the content is transferred to the receiver.

ICN has some similarities and differences with other related technologies like distributed database (DDB), data grids, peer-to-peer networks (P2P), content distribution networks (CDN), and cloud computing [4], [5]. ICN is considered as a new architecture in terms of naming, routing, caching, and security.

One of the major components in the new paradigm is the "security" component. ICN changes the security model from securing the path to securing the content, which is available to all ICN nodes. As a consequence, new attacks have appeared with this new security model in addition to the legacy attacks that may have an impact on ICN. The security in ICN will be an integral part of the architecture rather than added as an overlay.

This paper investigates the attacks in ICN, with a focus on the classifications of these attacks and the relation with unique ICN attributes and security requirements. This survey paper addresses the following primary points:

A Taxonomy of ICN Attacks: To the best of our knowledge, this paper proposes the first taxonomy of ICN attacks that classifies these attacks into four categories: naming, routing, caching, and other miscellaneous related attacks. Then it classifies the attacks in each category based on the types of the attacks.

Relation Between Unique ICN Attributes and ICN Attacks: We study how attackers benefit from the unique ICN attributes (location independent naming, state decorrelation, in-network caching, and ubiquitous publication/subscription) to perform their attacks.

Relation Between Security Requirements and ICN Attacks: We address how each ICN attack affects the security requirements: confidentiality, integrity, availability, and privacy.

Severity Levels of ICN Attacks: We calculate the severity level for each ICN attack based on the following evaluation metrics: block content retrieval, access user request, cache pollution, misrouting, request timeout, number of affected nodes, geographical distribution of attacked networks, remote exploitation, availability of attacked environment, and difficulty level of fixing damage. The calculation is based on the assumption that there is no explicit security mechanism used to defend against such attacks.

Existing ICN Security Solutions: We compare and contrast the existing ICN security solutions, which seem to be quite limited and require improvement.

Manuscript received January 16, 2014; revised June 19, 2014 and September 30, 2014; accepted December 9, 2014. Date of publication January 14, 2015; date of current version August 20, 2015. This work was supported in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada and in part by Bell Canada.

The authors are with the School of Computing, Queen's University, Kingston, ON K7L 3N6, Canada.

Digital Object Identifier 10.1109/COMST.2015.2392629

The survey presented in this paper can aid to answer many important questions, which summarize our major contributions as follows:

- What are the most important attacks that may take place in an ICN environment?
- How do unique ICN attributes relate to ICN attacks?
- What are the most important security requirements in ICN?
- What are the most severe ICN attacks?
- Why do we need new security solutions in ICN architectures?

The reminder of the paper is organized as follows. Section II discusses what makes ICN unique with respect to host-centric architectures. Section III presents a taxonomy of ICN attacks. Section IV shows the relations between ICN attacks and unique ICN attributes. Section V discusses ICN attacks with respect to security requirements. Section VI presents the severity level of ICN attacks. Section VII discusses existing ICN security solutions. Finally, Section VIII draws conclusions.

II. What Makes ICN Unique?

The idea of ICN started in the TRIAD project in 2000 [6], after which a number of research projects appeared. The most widely discussed ICN projects are Data Oriented Network Architecture (DONA) [7], Network of Information (NetInf) [8], Named Data Networking (NDN) [9] and Publish Subscribe Internet Technology (PURSUIT) [10]. DONA uses a flat and self-certifying naming system combined with a name resolution infrastructure that is organized in a hierarchical manner. Routing is performed using the route by name paradigm that is added as an overlay above the IP layer. NetInf uses a naming system similar to DONA with a name resolution service called Multilevel Distributed Hash Tables (MDHT) [11]. NDN uses a naming system that is composed of multiple hierarchical components; each component is a string of any length. There are two key messages in NDN, interest and data, which are also routed using a route by name paradigm. PURSUIT also employs a naming system similar to DONA. PURSUIT proposes a clean slate routing architecture for ICN that aims to shift the existing send-receive based Internet model towards a publish-subscribe model [12].

All ICN architectures have some generic concepts, which can be classified as follows: information object, naming, routing, caching, security, and application programming interface.

Information Object: Information object refers to the content itself, which is the main focus of ICN, regardless of its storage location and physical representation. For each content, there may be different representations and different copies for each representation.

Naming: The naming schemes in ICN can be classified into three categories: hierarchical, self-certifying, and attribute-value pair based. In hierarchical naming, names are composed of multiple hierarchical components. A component can be any string of any length that is generated and assigned by users. The names in this category are human friendly but non-persistent. In self-certifying naming, names consist of two parts of the form $P : L$ and metadata. The first part, P is the cryptographic hash of the owner's public key. The second part, L is a content label assigned by the owner. Meta-data contains the full public key and digital digest signed by the owner. Self-certifying names are unique, persistent, not limited to any organization and easy for integrity checking. In attribute-value pair based, each attribute has a name, a type and a set of possible values, but the names in this scheme do not ensure uniqueness or security for content names [13], [14].

TABLE I
Host-Centric Versus ICN

	Host-centric	ICN
Naming	define host topological position	define content regardless of its location or representation
Routing	between hosts using IP addresses	using name resolution entity or name-based routing
Caching	specific caching points (cache servers)	each node can cache any content passing through it
Security	secure communication channels between hosts	secure the content itself
API	send data to a specific address	publish and subscribe contents

Routing: In ICN, routing techniques can be classified into two major approaches: name resolution and name-based routing. Name resolution involves two steps. In the first step, the content name is resolved to a single or a set of IP addresses. In the second step, using any topology based on shortest path routing like Open Shortest Path First (OSPF), the request is routed to one of these IP addresses. In the process of name-based routing, a request is routed directly based on the content name and state information is stored along the way, so that the content itself can be delivered using the reverse path to the receiver [15].

Caching: In-network caching in ICN achieves the following principles: uniform, i.e., applied to all content delivered by any protocol; democratic, i.e., published by any content providers; and pervasive, i.e., available to all network nodes [16].

Security: In the ICN architecture, as the network and/or user can use any available copy, security cannot be bound to the endpoints or storage location like a host-centric architecture. Consequently, new information-centric security concepts are required that let the security be applied on the content itself. Several ICN architectures integrate security aspects within the architecture itself not as an overlay on the routing layer.

Application Programming Interface (API): An API in ICN is used to request and deliver the content. The source publishes its content to make it available for other users in the network. A user sends a subscription message for the content that he/she is interested in. The two operations (publish and subscribe) use the content name as the prime parameter.

Table I summarizes the important differences between host-centric and ICN architectures in terms of naming, caching, routing, security, and application programming interface. Fig. 1 shows the basic operation of an ICN network.

In addition to the preceding concepts, ICN as a solution for the upcoming Internet era should also achieve the following design principles [17], [18]:

- **Scalability**. Serve a very large number of entities.
- **Availability**. Ensure that the network has a usable operation rate.

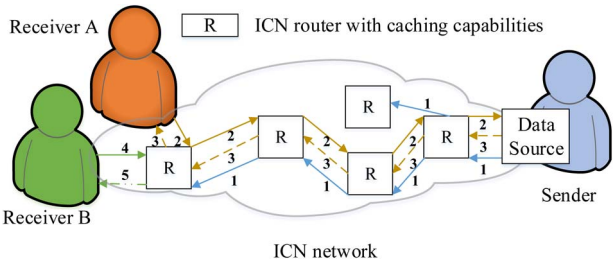

Fig. 1. ICN basic process: 1- Publish message: A sender sends a publication message with the content name to the ICN network. 2- Subscribe message from receiver A: A receiver sends a subscription message with the content name to the ICN network. 3- Delivery path for receiver A: The ICN network builds a delivery path from the data source to the receiver. 4- Subscribe message from receiver B: Another receiver sends a subscription message for the same content. 5- Delivery path for receiver B: The ICN network delivers the content from the closest available copy via the ICN in-network caching.

- **Reliability**. Easily recover in case of any failures.
- **Network management simplicity**. Support self-configured and self-optimized networking.
- **Quality of Service (QoS)**. Develop prioritization criteria for contents that allow the network to provide content-based QoS.
- **Loosely coupling system**. Provide more flexibility in time constraints, sequencing, and environment assumptions.
- **Flexible business models**. Allow and encourage different stakeholders to share and participate with their contents in the ICN open environment.

From the security point of view, ICN has five attributes that make it unique with respect to other related technologies. First, there is no host identifier in ICN architectures that makes it difficult to apply limits on user requests. Second, any user can use any available copy from any location that adds difficulty to authorize user access. Third, any user can publish/subscribe any content that allows attackers to make fuzzy publications/subscriptions. Fourth, the network nodes see the requests, which adds more risk of losing privacy than before. Fifth, the security in ICN will be an integral part of the architecture and not as an overlay as is common in host-centric architectures.

III. Taxonomy of ICN Attacks

ICN has many security issues to be addressed. There are new types of attacks in ICN that did not occur before or did not have any significant impact in other environments. Additionally, many attacks that occur in other environments may also appear in ICN environments [19]–[24]. This taxonomy classifies ICN attacks (new and legacy) into four categories as shown in Fig. 2: naming, routing, caching, and other miscellaneous related attacks. This classification depends on the attacker's *main* target. Although each attack is included in only one category, it may impact other categories as well. For example, both flooding and unpopular request attacks affect ICN routing and caching. In a flooding attack, the attacker's main target is to overload and exhaust routing resources and as a consequence it affects the caching system. In unpopular requests, the attacker's main target is to violate cache relevance and as a consequence it affects the routing system. The proposed categories are briefly introduced in the following four paragraphs:

Naming Related Attacks: ICN architectures face a greater threat with respect to the privacy as content requests are visible to the network. Many attackers try to censor/monitor Internet usage. An ICN architecture provides more access to user requests that would increase the attackers control on information flow and make blocking information much easier for them. In the naming related attacks in ICN, an attacker tries to prevent the distribution of a specific content by blocking delivery of this content and/or by detecting who requests this content [14], [25].

Routing Related Attacks: ICN content delivery depends on asynchronous publication and subscription, which adds extra effort to ensure consistency among distributed data states. Some attacks like jamming and timing aim to fail this state consistency, which may lead to unwanted traffic flows and/or denial of service. Other attacks, like infrastructure and flooding attacks, try to exhaust the resources like memory and processing power that are used to support, maintain and exchange content states. In addition, the infrastructure in ICN relies on the integrity and correctness of content routing, and is therefore threatened by poisonous injections of paths and names [26]–[30].

Caching Related Attacks: Caching is one of the important components in ICN as the performance of the ICN infrastructure is based on receiver driven caching that aims to deliver the closest available copy to a user. Therefore, ICN is vulnerable to all operations that pollute or corrupt the caching system [31]–[33].

Miscellaneous Attacks: The threats in this category aim to degrade some ICN services and allow an attacker to make unauthorized access. These attacks lead to insufficient or erroneous data distribution [34].

In the following subsections, we describe the attacks, scenarios, and impacts of each one of the four categories. The discussed attacks can also be classified as follows: new attacks in ICN such as bogus announcements and time analysis attacks; legacy attacks in new scenarios and with a greater impact in ICN such as naming and routing related attacks, random and unpopular requests in caching related attacks; legacy attacks with a different impact in ICN such as the other miscellaneous attacks.

A. Naming Related Attacks

The attacks in this category can be classified into watchlist and sniffing attacks. In ICN, the network nodes can access user requests. The attacker uses this attribute in addition to location independent naming to perform these types of attacks. There is a generic assumption that the attacker who compromises an ICN node or router can access it and monitor requesters [25]. In an ICN, there is no host identifier; hence an attacker needs to compromise an ICN node in order to track requesters and record who requested what. For content filtration and/or deletion attack, this assumption is not required at all.

Watchlist: An attacker has a predefined list of content names that he/she wants to filter or delete. Then the attacker monitors network links to perform a real-time filtering. The attacker may delete the request and/or record requester's information, in case of any matching against the predefined list. In addition, the attacker may try to delete the matched content itself. As depicted in Fig. 3, the attacker captures user requests to filter and record who requested what. The attacker also filters and records return

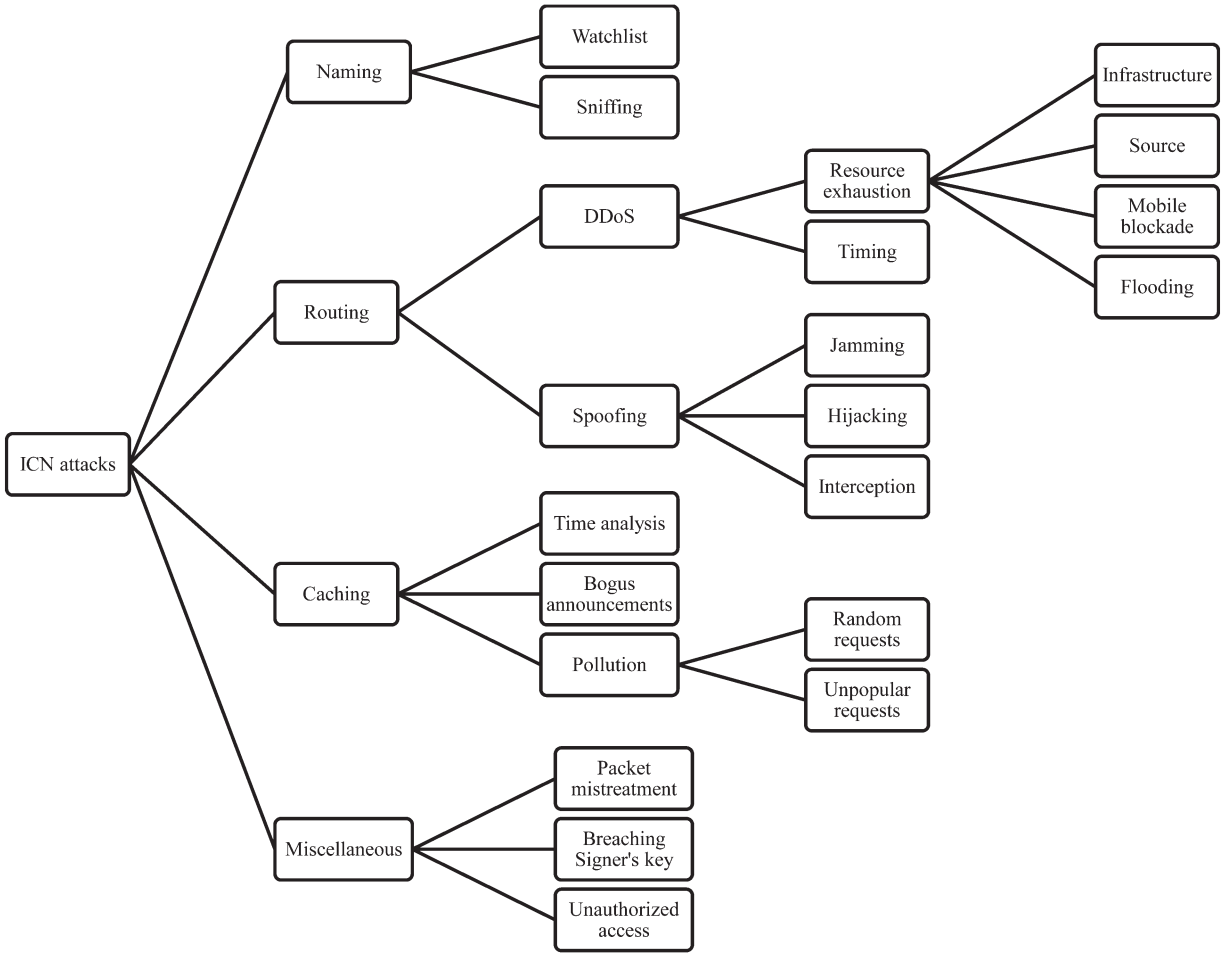

Fig. 2. Taxonomy of ICN attacks.

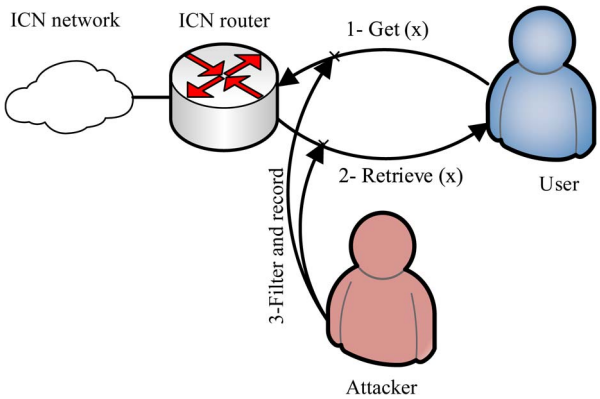

Fig. 3. Watchlist attack: 1- A user requests for ICN content named (x). 2- Normally, the user should retrieve the content (x). 3- An attacker can filter and record the requests and/or the contents based on his/her predefined list.

contents, which contain information about the publisher and the data. The filtration is based on the attacker's predefined list.

Sniffing: Unlike the predefined list in the watchlist attack, the attacker monitors the network to check the data if it should be marked in order to filter or eliminate it. The data should be marked if it contains the specified keywords. The attack scenario is the same as the watchlist attack. The main difference is that the attacker does not have a predefined list, but he/she makes some analysis on requests or on the content.

Naming related attacks have an impact on the following:

- **Censorship**. Using the naming related attacks, an attacker can censor the contents that he/she wishes.
- **Privacy**. Using these types of attacks, an attacker can monitor the content requests of a large number of users and knows about the requesters. The ICN network accesses the user's requests, which results in a worse privacy situation.
- **Denial of service**. An attacker prevents user's requests for the marked content, leading to unanswered requests.

B. Routing Related Attacks

The attacks in this category can be classified into distributed denial of service (DDoS) and spoofing attacks. The DDoS attacks can be classified into resource exhaustion and timing attacks. Resource exhaustion can be categorized into infrastructure, source, mobile blockade, and flooding attacks. Spoofing attacks can be divided into jamming, hijacking, and interception attacks.

Infrastructure: An attacker sends a large number of requests for available/unavailable content. As ICN architectures try to find the closest copy from the best available location, these requests take different routes towards the source causing overload conditions. If the number of these requests is significantly high, it leads to a denial of service. This attack may be further amplified, as regular users send retransmission requests after a

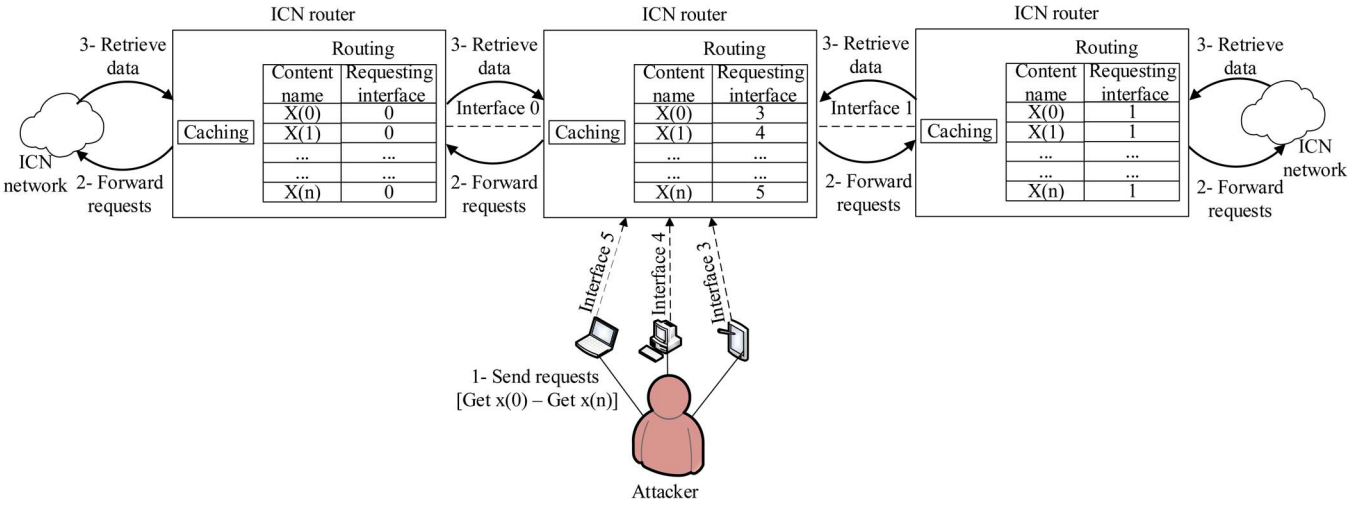

Fig. 4. Infrastructure attack: 1- An attacker, who controls many end systems, sends a large number of requests to ICN routers. 2- The attacked routers forward these requests to the neighboring routers, and in turn they send it to their neighboring routers and so on. 3- ICN starts to retrieve these large amounts of data from different paths and sends it back to the requested locations.

specified time. Similar to the hijacking attack, this threat can be mitigated because routing mechanisms in ICN attempt to route towards multiple locations. As illustrated in Fig. 4, the attacker, who controls many end systems, sends a large number of requests to one or more ICN routers to fill the routing table and exhaust processing and memory resources. As a consequence, the attacked routers forward these requests to the neighboring nodes, which in turn forward it to the next neighboring nodes and so on. If the number of invalid requests is so high, any legitimate request takes a longer response time. Consequently, if the response time exceeds the request timeout period, then the request may not be answered. This scenario can lead to denial of service or at least long delays.

Source: In ICN, attacking a single source may also lead to overload conditions for the routing infrastructure. An attacker sends a large number of requests to a specific content source to degrade its performance. As a consequence, this attack increases the response time of content delivery for this content source or its access router. In addition to this effect, the attack can lower the data return rate and affect requests of all nodes in the paths to receivers. The attack scenario is similar to the infrastructure attack scenario. This attack not only affects the attacked source, but also affects the overall network.

Mobile Blockade: A mobile attacker can overload a region by traversing neighboring networks on circular paths while sending a significant number of content requests. The attacker aims to overload the mobile access routers to make it exceed the state timeout that leads to a blockade of the regionally available networks. The retransmission of requests is part of the mobility aspect in an ICN environment that adds difficulty in detecting this attack [35]. The attack scenario presented in Fig. 5 is similar to the infrastructure attack scenario. The difference is that the mobile attacker sends a high number of requests to neighboring networks, whereas the attacker is traversing between the networks in a circular and continuous manner.

Flooding: The existing solutions for flooding attacks in ICN are designed to limit the number of requests, which are not appropriate for ICN [27], [36], [37]. An attacker can send a large number of requests that exceeds this limit. The attacked node accepts a certain number of requests and then ignores the remaining requests. As a consequence, the attacker succeeds to overload the overall infrastructure and harms all proximate users. Additionally, as ICN is a content centric architecture, it is difficult to apply limits for request rate per end user because there is no host identifier. The attack scenario is also similar to the infrastructure attack scenario. The difference is that the attacker sends a number of requests that exceeds the limits of the ICN nodes, and therefore ICN neglects the legitimate requests directed to the attacked nodes.

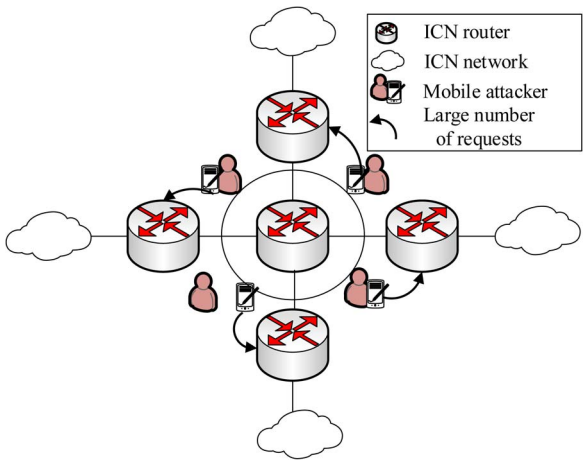

Fig. 5. Mobile blockade attack: A mobile attacker sends a large number of requests, while he/she is traversing ICN neighboring networks.

Timing: This refers to increasing the request timeout for some ICN nodes to violate the consistency between the ICN asynchronous publication and the subscription process. An attacker sends a large number of requests to degrade the performance of some routers, so that request routing and data forwarding exhibit longer delays. The attack scenario is also similar to the infrastructure attack scenario. The difference is that the attacker sends a large number of requests through one or more routes to increase the request timeout for legitimate user's requests.

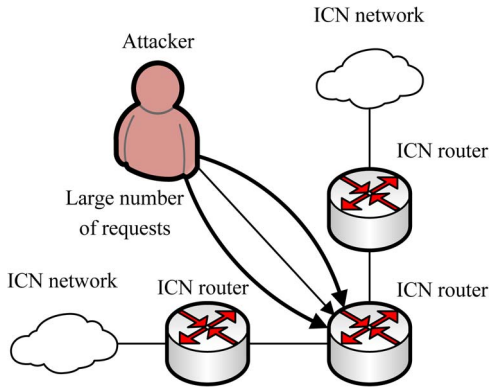

Fig. 6. Jamming attack: An attacker sends a large number of requests to a shared node.

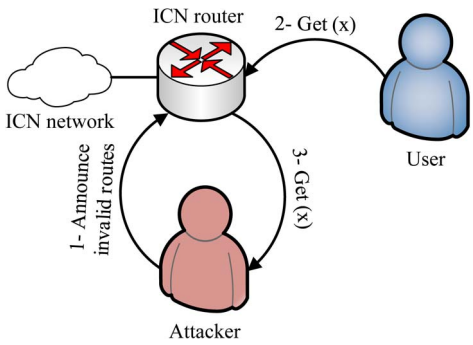

Fig. 7. Hijacking attack: 1- An attacker announces invalid routes for some content including (x). 2- A user requests for ICN content named (x). 3- ICN router redirects the user's requests to the attacker's malicious routes, and consequently the user does not get any response.

Jamming: A node on a shared link sends a large number of malicious unnecessary content requests. The attacker who masquerades as a trusted subscriber sends the malicious requests to disrupt the information flow in the system. The ICN network replies and the content is sent to the destination without a receiver. This attack scenario is similar to the infrastructure attack scenario. The difference, as presented in Fig. 6, is that the attacker sends requests to a shared node, which forwards it to neighboring nodes.

Hijacking: Unlike host-centric architectures, any node in ICN can cache and publish/subscribe contents. An attacker who masquerades as a trusted publisher may announce invalid routes for any content. Content requests from users in the proximity of the attacker are directed towards these invalid routes. Consequently, these requests will be unanswered, which lead to a DoS. The effect of this attack may be exacerbated, if the attacker has the ability to hijack invalid routes on a large scale. The effect of this attack is lessened because the routing mechanisms in ICN attempts to route towards multiple locations. As depicted in Fig. 7, the attacker announces invalid routes for some contents to attract the user requests. When legitimate users send requests for one of these malicious routes, ICN nodes forward these requests to the malicious nodes. Consequently, the legitimate user does not receive a response.

Interception: This attack is similar to the usual "man in the middle" attack. Unlike a hijacking attack, an attacker who masquerades as a trusted publisher announces invalid routes, while

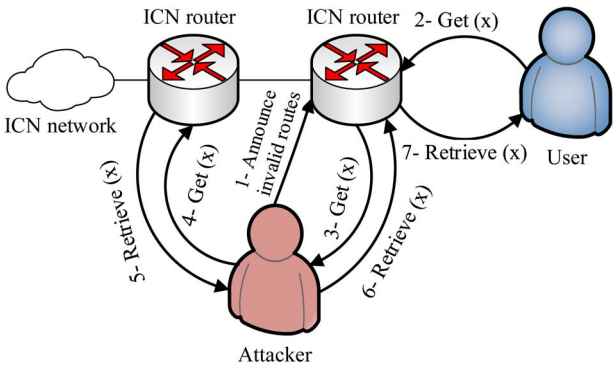

Fig. 8. Interception attack: 1—An attacker announces invalid routes for some content including (x). 2—A user requests for ICN content named (x). 3—ICN router redirects the user request to the attacker's malicious routes. 4—The attacker forwards the request to get the actual content. 5—The attacker retrieves the content (x). 6—The attacker forwards the content to the requested user. 7—The user retrieves the content (x).

maintaining a record of valid routes to the content. Content requests can then be captured and sent to the proper location. Although the receiver gets the content normally, the attacker gains knowledge of the requested content. As shown in Fig. 8, the attacker announces invalid routes for some contents to attract the user's requests. When legitimate users send requests for one of the malicious routes, ICN nodes forward these requests to the attacker's malicious node. The attacker records who requested this content and then forwards it to get the actual data. When the actual data arrives to the attacker's node, the attacker forwards it back to the requested ICN node, which in turn forwards it to the legitimate user. For the user, the scenario seems to be normal, but actually the attacker violates the user's privacy.

Routing related attacks have an impact on the following:

- **Denial of service**. DoS may occur due to many attacks in this category, such as sending many requests for unavailable contents or to a single source, mobile blockade, flooding, hijacking, and timing. Consequently, intermediate timers delete requests with the expired timeouts, which may lead to DoS or at least long delays.
- **Resource exhaustion**. There are many sources for resource exhaustion in the ICN infrastructure that come from misuse or uncontrolled traffic such as sending a large number of requests and flooding attacks.
- **Path infiltration**. In ICN, copies of content are typically distributed to many untrusted locations, and therefore it is difficult to authenticate valid origins for contents. Hijacking and interception are the major sources of path infiltration in ICN as attackers may announce invalid routes and claim them as trusted ones.
- **Privacy**. The privacy violation in the interception attack gives the attacker unauthorized access to user's requests especially when the attacker is topologically close or on the route to the user.

C. Caching Related Attacks

The attacks in this category can be classified into time analysis, bogus announcements, and cache pollution attacks. The cache pollution can be classified further into random and unpopular request attacks.

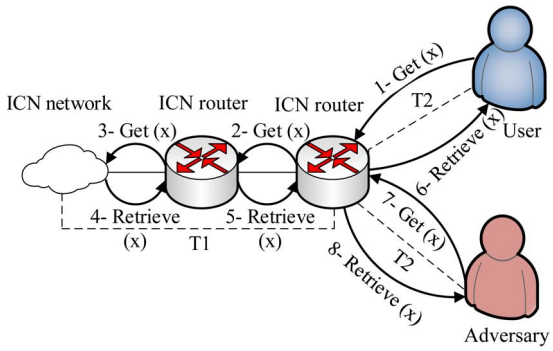

Fig. 9. Time analysis attack: 1—A user requests for ICN content named (x). 2 and 3—ICN routers try to find the content (x). 4 and 5—ICN routers forward the content (x) to the requested user. 6—The user retrieves the content (x) in total time $T_1 + T_2$. 7—An adversary requests for the content (x). 8- The adversary retrieves the content (x) in time T_2 only, as routers cache the content.

Time Analysis: In ICN, any node can potentially cache any content. An adversary measures the time difference between request response times for cached and uncached content. This difference can be used to conclude if a proximate user has previously requested the same content as the requested one by the adversary. This attack violates the user's privacy as the adversary can gain information about this proximate user. As depicted in Fig. 9, T_1 is the time required to send the request and receive data between the content source and the closest router to the user or the adversary, and T_2 is the time required to send the request and receive data between the user or the adversary and the closest router. When a legitimate user requests a certain content, the ICN infrastructure forwards the request to the content source and returns the data to the user in a total time of $T_1 + T_2$. Then if the adversary requests the same content, he/she gets it in time T_1 as there is already a cached copy of the content. The adversary uses this time difference to know if a proximate user requested this content before or not.

Bogus Announcements: As the caching system is a major part of the ICN architecture, an attacker can send many announcement updates for content or cached copy at a frequency that exceeds the local content request routing convergence time, to violate the caching and routing systems. As a consequence, an ICN will not be able to match the legitimate requests in the existence of these network quick updates. These overloaded announcements lead to incomplete and erroneous content retrieval as illustrated in Fig. 10.

Random Requests: An attacker aims to spoil the ICN in-network caching system and to change the content popularity. The attacker forces ICN caches to store unpopular contents by sending random requests for these unpopular contents. An unpopular content refers to a content that is not frequently requested. Alternatively, the attacker may request false contents to fill the caches with invalid contents. A content is fake if it is modified or does not come from the intended source, or it is not the content requested by the user. As shown in Fig. 11, in the normal case, if a second user requests a cached copy, he/she gets the data from the closest available location as the caching system caches each content passing through it. As shown in Fig. 12, in the attacked case, the attacker sends a massive number of random requests to spoil the caching system. In the latter case, if the second user requests the same content, his request takes the full path as the first user.

Unpopular Requests: An attacker only requests unpopular contents to spoil the ICN in-network caching and changes the content popularity. This attack requires a prior knowledge of the content popularity. The attack scenario has similar effect as the random requests case.

Caching related attacks have an impact on the following:

- **Privacy**. The caching mechanism in ICN is uniform, democratic and pervasive, which causes a greater privacy risk than in current architectures. As in the time analysis attack, the adversary can know whether a proximate user has previously requested this content or not and that violates user's privacy.
- **Denial of service**. Bogus announcements cause many updates to contents that lead to incomplete or erroneous data states. The mapping system will not be able to process these updates and, as a consequence, users do not retrieve the required contents.
- **Cache pollution**. Any user in ICN can send many random and/or unpopular requests that cause cache pollution [38].

D. Miscellaneous Attacks

The other miscellaneous attacks can be classified into packet mistreatment, breaching signer's key and unauthorized access attacks.

Packet Mistreatment: This refers to normal active network attacks during data transmission that also includes the replay attacks. An attacker, who has access to a link fraudulently or maliciously, tries to block, change, or reply to requested data many times. In this attack scenario, the attacker accesses ICN nodes or network links to do the following: modify packets during transmission, reply to requester multiple times, or generate content on behalf of a legitimate user.

Breaching Signer's Key: An attacker can use any common attack to breach the signer's keys. This problem with ICN has a greater impact as publishers sign contents that are available for a long time and in large volumes. As shown in Fig. 13, the attacker retrieves specific contents to break the signer's key. The data contains publisher public information and signature. This data may be large enough to simplify the attacker's task to get the signer's key.

Unauthorized Access: An attacker can access a certain content sent to a specific user or group of users that he/she is not allowed to access. In ICN, unauthorized access attacks become easier because an attacker can use any available copy for a content, which is distributed in different network locations.

Miscellaneous attacks have an impact on the following:

- **Congestion**. The attacker redirects the packets to heavily loaded links, which can lead to congestion in the network. In addition, packet mistreatment attacks can result in lowering of the connection throughput.
- **Denial of service**. The attacker sends a large number of packets toward a source or network entity causing DoS using packet mistreatment attacks.
- **Masquerading**. The attacker claims that he/she is a trusted entity. If the attacker succeeds to get the signer's

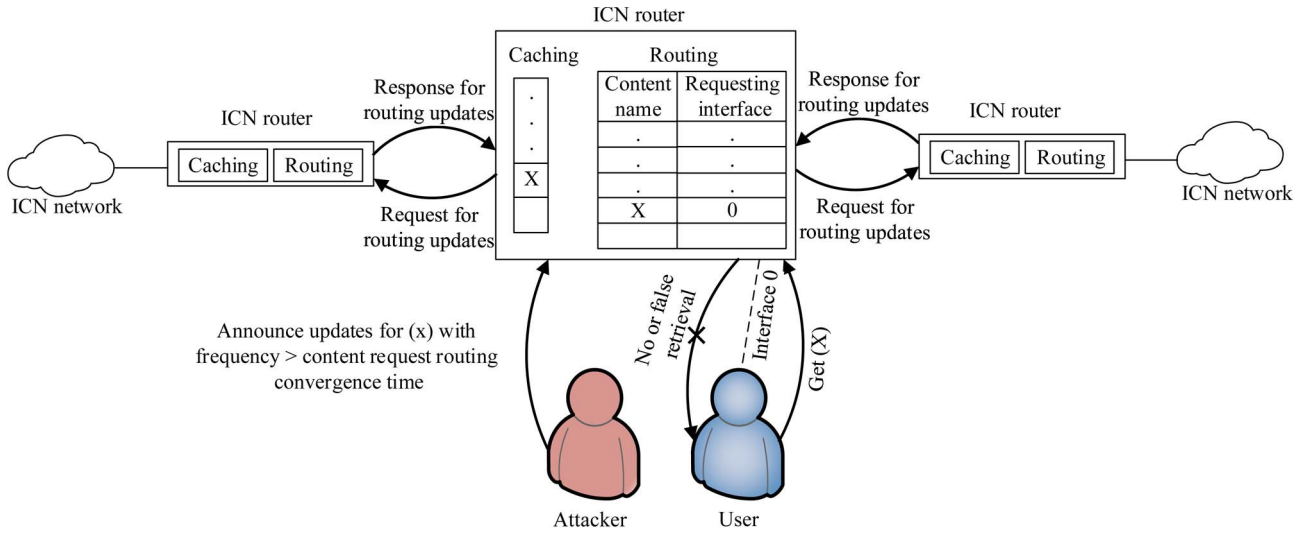

Fig. 10. Bogus announcements attack: A user requests for ICN content named (x), while an attacker sends a large number of updates for contents including (x), with a frequency that exceeds content request routing convergence time. ICN routers will not be able to update its routing table because of these bogus announcements, which lead to no or false content retrieval.

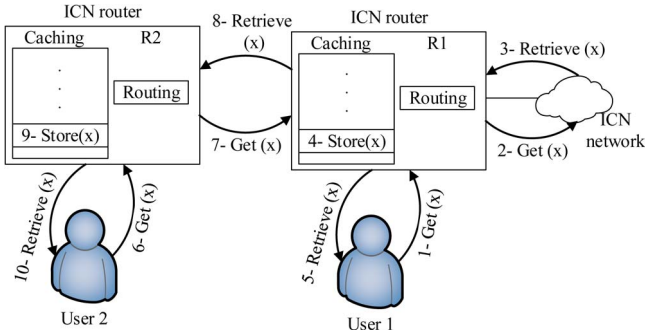

Fig. 11. Random requests attack (normal case): 1—User1 requests for ICN content named (x). 2—R1 router tries to find the content (x). 3—R1 retrieves the content from ICN network. 4—R1 caches the content (x). 5—User1 retrieves the content (x). 6—User2 requests the same content (x) via R2 router. 7—R2 tries to find the closest copy, which exists in R1 router. 8—R1 sends the content to R2 router. 9—R2 caches the content (x). 10—User2 retrieves the content (x).

key, then he/she can intercept, analyze, and/or corrupt the communications.

- **Unauthorized access to data**. In ICN, routers have direct access to content requests. Therefore, if the attacker succeeds to hack a router, then he/she is able to monitor the requests submitted by the users. This allows the attacker to discover user requests and monitor the user's daily life. For example, the attacker might track a certain user by capturing his/her requests.

IV. ICN Attributes Affecting Security

We identify four attributes, which may increase the impact of attacks in the ICN. By using these attributes, the attackers may be able to focus on the attacks that have more consequence or are harder to detect or prevent in ICN. These attributes are as follows:

- **Location independent naming**. This attribute allows content retrieval from multiple unknown or untrusted locations. ICN requires a secure naming system to name contents regardless of its location and representation.
- **State decorrelation**. ICN has two asynchronous states: request routing and content delivery. ICN requires consistency between these two states. Failures in the state consistency may lead to DoS or unwanted traffic problems.
- **In-network caching**. Caching is one of the prominent characteristics of ICN architectures. Any node of the network can cache any item that passes through it. The content can be delivered from the closest cache that contains the content instead of going to the hosting server.
- **Ubiquitous publication/subscription**. Any user can access ICN network from any location and act as content suppliers or content consumers. Some users may send unwanted contents or requests.

Table II shows the relation between ICN attacks and these ICN attributes. In this table, we show how an attacker can benefit from these attributes to achieve each attack. There are two values: P for primary attribute; and S for secondary attribute. These values indicate how much the attacker uses each attribute in each attack (P: an attacker depends completely on this attribute and the attack cannot happen without this attribute; S: an attacker depends partially on this attribute and uses it as an aid for an attack).

V. ICN Attacks vs. Security Requirements

Because of the nature of the ICN architectures, ICN has greater privacy and availability risks than current networking paradigms, and there is an urgent need for a new security solution that is capable of detecting and preventing all these attacks. The solution must achieve the four security requirements: confidentiality, integrity, availability, and privacy. Confidentiality indicates that only eligible entities can access secured information. Data integrity means the ability to identify any accidental or intentional changes to information objects and the corresponding metadata. Availability ensures that the objects published in the network have to be available and accessible for authorized entities. Privacy represents the protection of users

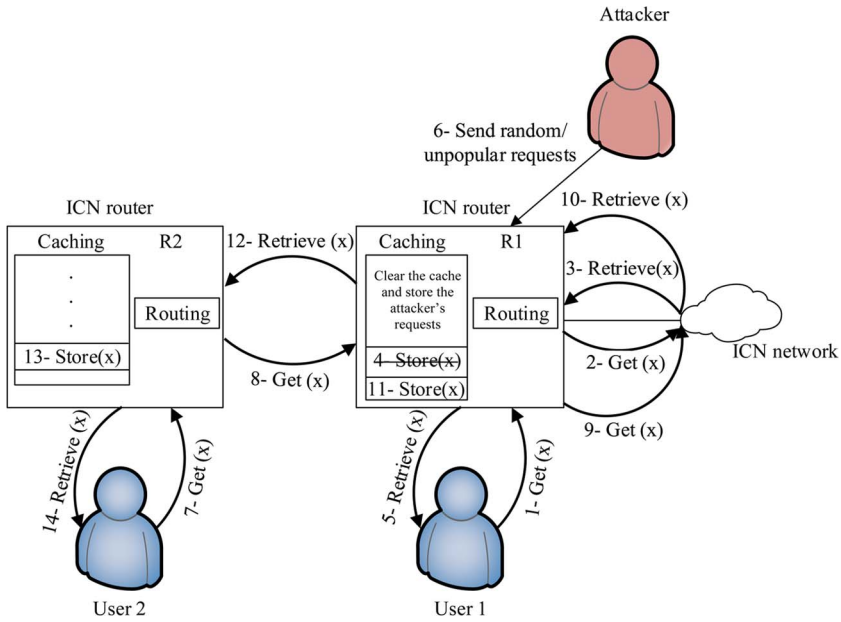

Fig. 12. Random requests attack (attacked case): 1—User1 requests for ICN content named (x). 2—R1 router tries to find the content (x). 3—R1 retrieves the content from ICN network. 4—R1 caches the content (x). 5—User1 retrieves the content (x). 6—An attacker sends a large number of random/unpopular requests to violate the cache. 7—User2 requests the same content (x) via R2 router. 8—R2 tries to find the closest copy and sends request to R1. 9—R1 router tries to find the content (x). 10—R1 retrieves the content from ICN network. 11—R1 caches the content (x). 12—R1 sends the content to R2. 13—R2 caches the content (x). 14—User2 retrieves the content (x).

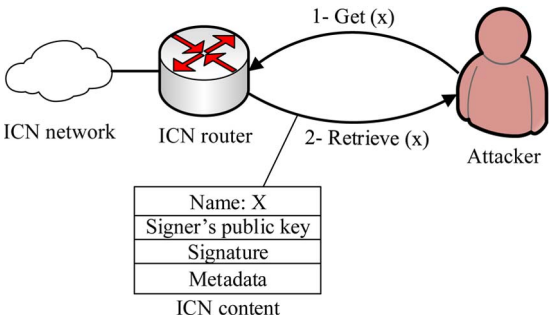

Fig. 13. Breaching signer's key attack: 1—An attacker requests for ICN content named (x). 2—The attacker retrieves the content (x) that contains signer's public key and signature, which can be used with the content itself to determine the signer's key.

as well as contents. Table III shows the relation between ICN attacks and security requirements. In this table, we show the effect of each attack on the security requirements using the OWASP risk rating [39]. The following values are used: H for high, M for medium, and L for low.

- **Confidentiality** (data disclosure and sensitivity). H: all data affected; M: extensive data affected; L: minimal data affected.
- **Integrity** (data corruption). H: all data affected; M: extensive data affected; L: minimal data affected.
- **Availability** (service loss). H: all services affected; M: extensive services affected; L: minimal services affected.
- **Privacy** (reveal of personal identifiable information). H: any user; M: proximate users; L: one individual.

VI. Severity of ICN Attacks

According to severity assessment by Symantec [40], we define ten metrics to evaluate the severity level of each attack.

TABLE II
ICN Attributes Affecting Security
(P: Primary; S: Secondary; Blank: No Impact)

Attack	Location independent naming	State decorrelation	In-network caching	Ubiquitous publication/ subscription
Watchlist	P			
Sniffing	P			
Infrastructure		P	S	P
Source		S	S	P
Mobile blockade		S	S	P
Flooding		S	S	P
Timing		S	S	P
Jamming		S	S	P
Hijacking	P		S	P
Interception	P		S	P
Bogus announcements	S	P	P	P
Random requests		S	P	P
Unpopular requests		S	P	P
Time analysis			P	
Packet mistreatment		S	S	S
Breaching signer's key	S	P	S	S
Unauthorized access	S		P	S

Some of these metrics related to the ICN architecture such as block content retrieval, access user request, cache pollution, and request timeout. The other metrics generally evaluate the effect of each attack on the attacked environment. In assessing the severity of these attacks, we assume that there is no explicit security mechanism for these attacks for the ICN considered in

TABLE III
ICN ATTACKS VS. SECURITY REQUIREMENTS
(H: HIGH; M: MEDIUM; L: LOW; BLANK: NO IMPACT)

Attack	Confidentiality	Integrity	Availability	Privacy
Watchlist	L		L	H
Sniffing	L		L	H
Infrastructure			H	
Source			L	
Mobile blockade			L	
Flooding			M	
Timing			M	
Jamming			L	
Hijacking	L		L	
Interception	L			M
Bogus announcements			H	
Random requests			M	
Unpopular requests			L	
Time analysis				M
Packet mistreatment		H	M	
Breaching signer's key	H	H		H
Unauthorized access	M	M		

this paper. The severity level for each attack can be determined by the following metrics:

- **Block content retrieval**. H: blocks contents directed to any ICN user; M: blocks contents to neighboring network users; L: blocks contents to proximate user.
- **Access user request**. H: accesses requests from any ICN user; M: accesses requests from proximate users; L: accesses requests from specific users.
- **Cache pollution**. H: affects all cache entries; M: affects large number of cache entries; L: affects limited and small number of cache entries.
- **Misrouting**.
- **Request timeout**.
- **Number of affected nodes**.
- **Geographical distribution of attacked networks**.
- **Remote exploitation**.

The preceding five metrics are assessed as follows: H: attack targets/affects/controls large scale ICN networks; M: attack targets/affects/controls neighboring networks; L attack targets/affects/controls specific nodes.

- **Availability of attacked environment**. H: attacker has no constraints; M: attacker attacks certain locations; L: attacker should have some privilege or prior knowledge.
- **Difficulty level of fixing damage**. It depends on five attributes: misrouting, number of affected nodes, geographical distribution of attacked networks, remote exploitation, and availability of attacked environment. H: cannot recover from the impact if the attacker accesses private information or at least three of the five dependent attributes are high; M: at least three of the five dependent attributes are medium; L: anything else.

Table IV shows the severity level of ICN attacks, which can be classified into high, medium, and low severity. We calculate the severity for each attack by assigning a numeric value for each level (0 for no impact; 1 for low; 2 for medium; 3 for high). Then we sum the values for each attack and calculate the percentage of the attack severity. The final severity level is low if the attack has an effect of less than or equal to 30%; medium if the attack has an effect of more than 30% and less than or equal to 70%; and high if the attack has an effect of more than 70%. The final severity reflects the impact of each attack on the ICN environment. Fig. 14 shows the severity of each attack. The high severity attacks such as the infrastructure and bogus announcements mean that these attacks cause a catastrophic effect on the ICN environment because they can be performed in a distributed manner on a large scale networks and affect any users. The low severity attacks such as hijacking, time analysis, and breaching signer's key mean that these attacks cause a minor effect on the ICN environment because of their limited influence on the networks and users. In between, the medium severity attacks (e.g., watchlist, flooding, and random requests) refer to the attacks that cause a partial effect on the ICN environment.

VII. ICN SECURITY SOLUTIONS

In this section, we summarize existing security solutions for each category of ICN attacks.

Naming: Existing solutions for naming related attacks, such as mix-nets [41], Tor [42], Freedom [43], Anonymizer [44], Freenet [45], and deniable encryption [46], cannot be applied in ICN as they are not designed for environments in which content is the main focus of the architecture. They require other conditions that are not suitable in ICN like user sizable infrastructure, shared information between publisher and user, and specific storage infrastructure. The ICN security solution should achieve privacy, censorship resistance and plausible deniability for users. The solution should also be computationally easy for the users to retrieve the content and computationally expensive for the attackers to identify or detect the name requested or content retrieved. Arianfar *et al.* [25] present a generic solution for naming related attacks that does not require shared keys between the publishers and consumers. This solution makes several assumptions that may not be applicable in ICN. The solution does not provide ideal privacy and it is suitable only when there is a large number of users. Ion *et al.* [47] design an attribute-based encryption and routing privacy scheme for the ICN to support data confidentiality. The basic idea is to apply distributed access control policies to the contents and specify these policies in terms of the contents. This scheme supports large scale environments with no need to share keys. This scheme is tested only on NDN architecture, hence it needs to be tested in the other architectures. It also needs to address the effect of applying the control policies on the ICN scalability.

Routing: Existing solutions for routing related attacks [27], [48] propose rate limiting per end user, which is a difficult task as the ICN has no host identifiers and the attacker can easily create a large number of requests that exceed the specified limit. ICN has a greater risk and requires new solutions as the ICN depends on content states that can be created, modified or deleted by any user of the network [26]. Gasti *et al.* [27] present a high level classification of DDoS attacks and their solutions in the NDN architecture. Fotiou *et al.* [28] suggest a ranking

TABLE IV
ICN ATTACKS SEVERITY (H: HIGH; M: MEDIUM; L: LOW; BLANK: NO IMPACT)

Attack	Block content retrieval	Access user request	Cache pollution	Misrouting	Request timeout	Number of affected nodes	Geographical distribution of attacked networks	Remote exploitation	Availability of attacked environment	Difficulty level of fixing damage
Watchlist	H	H			L	L		L	H	H
Sniffing	H	H			L	L		L	H	H
Infrastructure	H		H	H	H	H	M	H	H	H
Source	L		L	L	L	L		M	L	L
Mobile blockade	L		L	L	L	L		M	L	L
Flooding	M		M	M	L	L	L	M	M	M
Timing	M		M	M	L	L	L	M	M	M
Jamming	L		L	L	L	L		M	L	L
Hijacking	L		L		L	L		L	L	L
Interception		M	L		L	L		L	L	H
Bogus announcements	H		H	H	H	H	H	H	H	H
Random requests			M	M	L	M	H	M	M	M
Unpopular requests			L	L	L	L	H	L	L	L
Time analysis		M			L	L		L	L	H
Packet mistreatment	L		M	M	M	M	L	M	M	M
Breaching signer's key					L			H		H
Unauthori-zed access		M			M	L		H	H	M

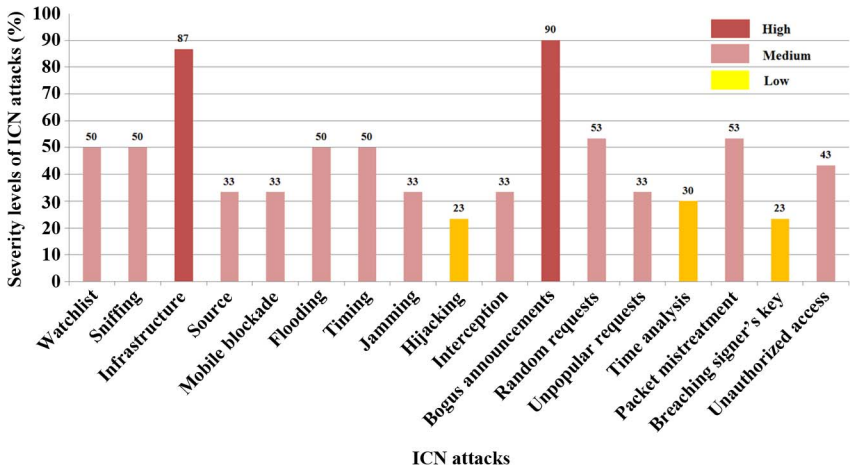

Fig. 14. Severity levels of ICN attacks.

algorithm for ICN contents to fight spam, which is based on publisher and subscriber rankings. Compagno *et al.* [29] present the concept of request flooding for unavailable contents. Afanasyev *et al.* [30] address the same attack by limiting the request rate with a constant function. The aforementioned solutions only work on a specific ICN architecture and each only addresses a specific type of DDoS attack.

Many papers classify DDoS attacks and their detection/prevention mechanisms [49]–[51]. The widely discussed countermeasures for DDoS in the Internet architecture are IP trace back [52], packet filtering [53], and rate limiting [54]. These techniques cannot be used in ICN as they depend on IP addresses for the end-points.

Caching: Existing solutions for caching related attacks are designed for a single cache server and are not suitable for ICN, as caching in ICN happens to all contents in all nodes. The ICN security solution should reduce the effects of these attacks on caching and store only the most frequently requested contents. The Cacheshield solution [31] handles random and unpopular requests for ICN caching. The suitability of Cacheshield in other ICN architectures and the scheme's scalability need to be evaluated. Mohaisen *et al.* [32] propose a privacy protection mechanism for the time analysis attack. The mechanism does not take into consideration different caching policies and assumes that the adversary is proximate to the attacked user. Ghali *et al.* [33] address content poisoning for ICN caching in the NDN architecture. They present a ranking algorithm based on the consumer feedback, which allows routers to distinguish between valid and malicious contents. Also there are many works for cache poisoning attacks as in the Domain Name System Security Extensions (DNSSEC) and the security solution for thwarting cache poisoning attacks in the DNS hierarchy (S-DNS) [55]. Such schemes depend on IP addresses of the end-points and hence are not suitable for ICN.

Miscellaneous Attacks: Existing solutions for the other miscellaneous attacks cannot be applied for ICN as a content has multiple copies distributed in different locations including replication servers and all caching nodes. An ICN security solution should verify the integrity of the document, verify the origin of the content, determine the consistency of the content obtained in relation to the requested one, and protect customer's privacy. Fotiou *et al.* [34] provide an access control mechanism for the unauthorized access attack, which includes an extra entity called access control policy (ACP). The suitability of the proposed access control mechanism in other ICN architectures and the scheme's scalability need to be evaluated.

There are other solutions designed for smart grid data collection that can be investigated for the ICN architectures. Kim *et al.* [56], [57] provide a scalable and secure transport protocol (SSTP) and end-to-end message protection proposed for the smart grid data collection. Smart grids handle massive amount of data generated from many measuring instruments. The suggested solutions are based on symmetric-key and provide lightweight implementation on both servers and clients. Kim *et al.* [58] propose a scalable, resilient, and secure platform (SeDAX) for the smart grid communications. This platform deals with high data volumes such as the expected data traffic in ICN. Vieira *et al.* [59] present a protocol that provides a secure overlay network for the ICN specially designed for smart grids. The key management in this protocol needs more investigations and the protocol needs to be tested with respect to the ICN scalability. There are also some interesting solutions for the web application attacks such as the ones suggested by Shahriar *et al.* [60], [61]. They propose server side and client side solutions that do not need information sharing between the client and the server.

We can conclude from the aforementioned solutions for smart grids and web applications that they can be used for ICN environments with some modifications. In ICN, it may be difficult to depend on shared key as any user can publish or subscribe any content. ICN also does not depend on the conventional client-server architectures and adding authentication servers may affect the ICN scalability.

Although security is a major concern in ICN, the research efforts so far are designed for a specific architecture or certain attacks. As indicated earlier in this paper, the security researchers have only scratched the surface of security issues in ICN and the research is in its early days. There is a need to develop new security solutions for ICN environment in an evolutionary manner based on appropriate security pattern classifications.

VIII. Conclusion

The future Internet comes with high requirements of information dissemination, which motivate the research community to find alternative solutions. ICN, as one of these solutions focuses on contents to provide a scalable and efficient content delivery. There are many proposals for ICN architectures like DONA, NetInf, NDN, and PURSUIT. ICN has attributes that make it unique from host-centric architectures. ICN mainly depends on location independent naming, in-network caching, and name-based routing.

This paper presents five major aspects relating to security in ICN. First, we develop a taxonomy of ICN attacks and classify the attacks into four categories: naming, routing, caching, and other miscellaneous related attacks. We describe each attack and the impacts of each category of ICN attacks. Second, we derive the relationships between ICN attacks and unique ICN attributes. We show for each attack how the attacker depends on the corresponding attributes to perform his/her attack. Third, we derive the relationships between ICN attacks and security requirements and discuss the impact of each attack on the requirements. Fourth, we calculate the severity levels for the attacks based on ten evaluation metrics. Fifth, we survey the existing ICN security solutions.

The attacks in an ICN environment can also be viewed from the following perspectives:

- New attacks in ICN environments. These include bogus announcements and time analysis attacks.
- Attacks that occur in non-ICN environments, but manifest themselves differently in ICN with new scenarios and a greater impact. These include naming and routing related attacks, in addition to random and unpopular requests in caching related attacks.
- Attacks that occur in both non-ICN and ICN environments in the same way but with a different impact. These are mentioned as "miscellaneous attacks" in this paper.

Based on the analysis of the relationships between attacks, ICN attributes and security requirements, availability and privacy are the most affected requirements in ICN architectures:

- **Availability**. Sending massive malicious requests to the routing or caching systems in ICN are the main sources that affect the availability in ICN.
- **Privacy**. Accessing the user's requests and the time difference between the cached and uncached content are the main impacting factors for the privacy in ICN.

Existing solutions target a specific architecture or specific types of attacks. Developing a generic and complete security solution that can be applied in any ICN architecture and integrated with the other technologies has become an urgent task for the ICN security. The major challenges for ICN security can be summarized as follows:

- Detection and prevention mechanisms for the attacks should be an integral component of the architecture. Security in ICN must be attached to the content itself, as the content may be distributed in different locations. Any user can use any available copy, which causes unauthorized access risks.
- There are higher privacy risks in ICN than typical host-centric environments. We present different types of attacks that can violate the privacy in ICN.
- Malicious publication/subscription is a risk as ICN is an open environment. We identify several ways where invalid requests can be sent to overload the ICN network and exhaust resources.
- It is difficult to limit requests per user in ICN as typically there is no identifier for a host.

REFERENCES

[1] *Cisco Visual Networking Index: Forecast and Methodology*, pp. 2012–2017, May 29, 2013.

[2] H. Moustafa and S. Zeadally, *Media Networks: Architectures, Applications and Standards*. Boca Raton, FL, USA: CRC Press, 2012.

[3] 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.

[4] A. M. K. Pathan and B. Rajkumar, "A taxonomy and survey of content delivery networks," Grid Comput. Distrib. Syst. Lab., Univ. Melbourne, Parkville, Vic, Australia, Tech. Rep., 2007.

[5] E. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 2, pp. 72–93, 2005.

[6] D. Cheriton and M. Gritter, "TRIAD: A scalable deployable NAT-Based Internet architecture," Stanford Univ., Stanford, CA, USA. [Online]. Available: http://ceng.anadolu.edu.tr/cakinlar/BIL555/icerik/2000-Triad.pdf

[7] T. Koponen *et al.*, "A data-oriented (and beyond) network architecture," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 4, pp. 181–192, Oct. 2007.

[8] "the network of information: Architecture and applications," SAIL, Brussels, Belgium, FP7-ICT-2009-5-257448-SAIL/D-3.1, Jul. 2011, accessed on 6 June 2014.

[9] V. Jacobson *et al.*, "Networking named content," in *Proc. CoNEXT*, Dec. 2009, pp. 1–12.

[10] D. Lagutin, K. Visala, and S. Tarkoma, "Publish/subscribe for Internet: PSIRP perspective," in *Towards the Future Internet*, vol. 4. Amsterdam, The Netherlands: IOS Press, 2010, pp. 75–84.

[11] M. D'Ambrosio, C. Dannewitz, H. Karl, and V. Vercellone, "MDHT: A hierarchical name resolution service for information-centric networks," in *Proc. ACM SIGCOMM Workshop ICN*, 2011, pp. 7–12.

[12] M. F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, and B. Mathieu, "A survey of naming and routing in information-centric networks," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 44–53, Dec. 2012.

[13] C. Tsilopoulos *et al.*, "A survey of information-centric networking research," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1024–1049, 2013.

[14] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–6.

[15] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Commun. Mag.*, vol. 49, no. 7, pp. 26–36, Jul. 2012.

[16] A. Ghodsi *et al.*, "Information-centric networking: Seeing the forest for the trees," in *Proc. 10th ACM Workshop Hot Topics Netw.*, 2011, pp. 1–6.

[17] *Future Internet Assembly*, accessed on Jun. 6, 2014. [Online]. Available: Available:http://www.future-Internet.eu/home/future-Internet-assembly.html

[18] F. Almeida and J. Loureno, "Information centric networks-design issues, principles and approaches," *Int. J. Latest Trends Comput.*, vol. 3, no. 3, pp. 58–66, Sep. 2012.

[19] D. Djenouri, L. Khelladi, and A. Badache, "A survey of security issues in mobile *ad hoc* and sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 4, pp. 2–28, 2005.

[20] M. L. Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 446–471, 2012.

[21] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 2009.

[22] V. M. Igure and R. D. Williams, "Taxonomies of attacks and vulnerabilities in computer systems," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 1, pp. 6–19, 2008.

[23] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 843–859, 2013.

[24] S. Hansman and H. Ray, "A taxonomy of network and computer attacks," *Comput. Security*, vol. 24, no. 1, pp. 31–43, Feb. 2005.

[25] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, "On preserving privacy in content-oriented networks," in *Proc. ACM SIGCOMM Workshop ICN*, Aug. 2011, pp. 19–24.

[26] M. Vahlenkamp, M. Whlisch, and T. C. Schmidt, "Backscatter from the data plane—threats to stability and security in information-centric networking," *Comput. Netw.*, vol. 57, no. 16, pp. 3192–3206, Nov. 2013.

[27] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS & DDoS in named data networking," in *Proc 22nd Int. Conf. Comput. Commun. Netw.*, 2013, pp. 1–7.

[28] N. Fotiou, G. F. Marias, and G. C. Polyzos, "Fighting spam in publish/subscribe networks using information ranking," in *Proc. 6th EURO-NF Conf. NGI*, Paris, France, Jun. 2010, pp. 1–6.

[29] 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.*, Oct. 2013, pp. 630–638.

[30] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *Proc. IFIP Netw. Conf.*, May 2013, pp. 1–9.

[31] M. Xie, I. Widjaja, and H. Wang, "Enhancing cache robustness for content-centric networking," in *Proc. IEEE INFOCOM*, 2012, pp. 2426–2434.

[32] A. Mohaisen, X. Zhang, M. Schuchard, H. Xie, and Y. Kim, "Protecting access privacy of cached contents in information centric networks," in *Proc. SIGCOMM*, Hong Kong, China, May 2013, pp. 1001–1003.

[33] C. Ghali, G. Tsudik, and E. Uzun, "Needle in a haystack: Mitigating content poisoning in named-data networking," in *Proc. SENT*, San Diego, CA, USA, 2014, pp. 1–10.

[34] N. Fotiou, G. F. Giannis, and G. C. Polyzos, "Access control enforcement delegation for information-centric networking architectures," in *Proc. 2nd Edition ICN Workshop Inf.-Centric Netw.*, Aug. 2012, pp. 85–90.

[35] G. Tyson, N. Sastry, I. Rimac, R. Cuevas, and A. Mauthe, "A survey of mobility in information-centric networks: Challenges and research directions," in *Proc. NoM*, New York, NY, USA, Jun. 2012, pp. 1–6.

[36] Y. You, M. Zulkernine, and A. Haque, "A distributed defense framework for flooding-based DDoS attacks," in *Proc. Int. Conf. AReS*, Barcelona, Spain, Mar. 2008, pp. 245–252.

[37] Y. You, M. Zulkernine, and A. Haque, "Detecting flooding-based DDoS attacks," in *Proc. IEEE ICC*, Glasgow, Scotland, Jun. 2007, pp. 1239–1234.

[38] Y. Gao, L. Deng, A. Kuzmanovic, and Y. Chen, "Internet cache pollution attacks and countermeasures," in *Proc. 14th IEEE ICNP*, Nov. 2006, pp. 54–64.

[39] *OWASP Risk Rating Methodology*, accessed on Jun. 6, 2014. [Online]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[40] *Symantec Security Response—Assessing the Severity of Threats, Events, Vulnerabilities, Security Risks*, Feb. 2006, accessed on Jun. 6, 2014. [Online]. Available: http://www.symantec.com/about/news/resources/press_kits/securityintelligence/media/SSR-Severity-Assesment.pdf

[41] D. L. Chaum, "Untraceable electronic mail, return addresses, digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, Feb. 1981.

[42] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proc. 13th USENIX Security Symp.*, 2004, p. 21.

[43] *Freedom System 2.0 Architecture*, accessed on Jun. 6, 2014. [Online]. Available: http://osiris.978.org/brianr/crypto-research/anon/www.freedom.net/products/whitepapers/Freedom_System_2_Architecture.pdf/

[44] Anonymizer, accessed on Jun. 6, 2014. [Online]. Available: http://www.anonymizer.com

[45] I. Clarke, T. W. Hong, S. G. Miller, O. Sandberg, and B. Wiley, "Protecting free expression online with Freenet," *IEEE Internet Comput.*, vol. 6, no. 1, pp. 40–49, Jan./Feb. 2002.

[46] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in *Proc. CRYPTO*, vol. 1294, *Lecture Notes in Computer Science*, 1997, pp. 90–104.

[47] M. Ion, J. Zhang, M. Schuchard, and E. M. Schooler, "Toward content-centric privacy in ICN: Attribute-based encryption and routing," in *Proc. ASIA CCS*, Hangzhou, China, Aug. 2013, pp. 513–514.

[48] C. Yi *et al.*, "A case for stateful forwarding plane," *J. Comput. Commun.*, vol. 36, no. 7, pp. 779–791, Apr. 2013.

[49] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, 2013.

[50] A. Keromytis, V. Misra, and D. Rubenstein, "SOS: An architecture for mitigating DDoS attacks," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 1, pp. 176–188, Jan. 2004.

[51] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, Apr. 2004.

[52] L. Lu, M. C. Chan, and E. C. Chang, "A general model of probabilistic packet marking for IP traceback," in *Proc. ASIACCS*, 2008, pp. 179–188.

[53] E. Kline, A. Afanasyev, and P. Reiher, "Shield: DoS filtering using traffic deflecting," in *Proc. 19th IEEE ICNP*, 2011, pp. 37–42.

[54] A. Mohaisen, X. Zhang, M. Schuchard, H. Xie, and Y. Kim, "A DoS-limiting network architecture," *ACM SIGCOMM CCR*, vol. 35, no. 4, pp. 241–252, Oct. 2005.

[55] H. M. Sun, W. H. Chang, S. Y. Chang, and Y. H. Lin, "DepenDNS: Dependable mechanism against DNS cache poisoning," in *Cryptology and Network Security*. New York, NY, USA: Springer-Verlag, 2009, pp. 174–188.

[56] Y. Kim, V. Kolesnikov, H. Kim, and M. Thottan, "SSTP: A scalable and secure transport protocol for smart grid data collection," in *Proc. IEEE SmartGridComm*, 2011, pp. 161–166.
[57] Y. Kim, V. Kolesnikov, and M. Thottan, "Resilient end-to-end message protection for large-scale cyber-physical system communications," in *Proc. 3rd IEEE SmartGridComm*, 2012, pp. 193–198.
[58] Y. Kim, J. Lee, G. Atkinson, H. Kim, and M. Thottan, "SeDAX: A scalable, resilient, secure platform for smart grid communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1119–1136, Jul. 2012.
[59] B. Vieira and E. Poll, "A security protocol for information-centric networking in smart grids," in *Proc. SEGS*, Berlin, Germany, Nov. 2013, pp. 1–10.
[60] A. Barua, H. Shahriar, and M. Zulkernine, "Server-side detection of content sniffing attacks," in *Proc. 22nd Annu. ISSRE*, Hiroshima, Japan, Nov. 2011, pp. 20–29.
[61] H. Shahriar and M. Zulkernine, "Client-side detection of cross-site request forgery attacks," in *Proc. 21st IEEE ISSRE*, San Jose, CA, USA, Nov. 2010, pp. 358–367.

Eslam G. AbdAllah (S'14) received the M.Sc. degree in computer systems from Ain Shams University, Cairo, Egypt, in 2010. He is currently working toward the Ph.D. degree with the School of Computing, Queen's University, Kingston, ON, Canada. He is a Member of the Telecommunication Research Laboratory and the Queen's Reliable Software Technology Group, School of Computing, Queen's University. His research interests include information-centric networks, network security, cryptography, and RFID.

Hossam S. Hassanein (S'86, M'91, SM'05) is the Founder and Director of the Telecommunications Research Laboratory, School of Computing, Queen's University, Kingston, ON, Canada, with extensive international academic and industrial collaborations. He is a leading authority in the areas of broadband, wireless and mobile network architectures, protocols, control, and performance evaluation. He is the author or coauthor of more than 500 publications in journals, conferences, and book chapters. Dr. Hassanein is a Senior Member of the IEEE and is a former Chair of the IEEE Communication Society Technical Committee on Ad Hoc and Sensor Networks. He is an IEEE Communications Society Distinguished Speaker (Distinguished Lecturer in 2008–2010). He has delivered numerous keynotes and plenary talks in flagship venues. He was a recipient of several Recognition and Best Paper Awards at top international conferences.

Mohammad Zulkernine (S'96, M'03, SM'09) received the Ph.D. degree from the University of Waterloo, Canada. He is a Canada Research Chair in Software Dependability and an Associate Professor with the School of Computing, Queen's University, Kingston, ON, Canada. He leads the Queen's Reliable Software Technology Research Group. He is also collaborating with various industrial research partners. His current research focuses on software reliability and security. Dr. Zulkernine is a Senior Member of the IEEE and the ACM, and he is a Licensed Professional Engineer in the Province of Ontario, Canada. He was one of the Program Cochairs of SSIRI'11, COMPSAC'12, and HASE'14. His research projects are supported by a number of provincial and federal research funding agencies.