2018 IEEE 16th Int. Conf. on Dependable, Autonomic & Secure Comp., 16th Int. Conf. on Pervasive Intelligence & Comp., 4th Int. Conf. on Big Data Intelligence & Comp., and 3rd Cyber Sci. & Tech. Cong.

A Security Framework for ICN Traffic Management

Eslam G. AbdAllah
Faculty of Computer and Information Sciences,
Ain Shams University
El-Abaseya, Cairo, Egypt
eslam_gamal@cis.asu.edu.eg

Mohammad Zulkernine, and Hossam S. Hassanein
School of Computing,
Queen's University
Kingston, Ontario, Canada
{*mzulker, hossam*}*@cs.queensu.ca*

***Abstract*—Information Centric Networking (ICN) changed the communication model from host-based to content-based to cope with the high volume of traffic due to the rapidly increasing number of users, data objects, devices, and applications. ICN communication model requires new security solutions that will be integrated with ICN architectures. In this paper, we present a security framework to manage ICN traffic by detecting, preventing, and responding to ICN attacks. The framework consists of three components: availability, access control, and privacy. The availability component ensures that contents are available for legitimate users. The access control component allows only legitimate users to get restricted-access contents. The privacy component prevents attackers from knowing content popularities or user requests. We also show our specific solutions as examples of the framework components.**

***Keywords*-Security framework; ICN; traffic management**

I. Introduction

According to Cisco Visual Networking Index 2016 and by 2020 [1], there will be almost 4.1 billion Internet users and 26.3 billion network devices and connections globally, the average fixed broadband connection speed will increase to 47.7 Mbps, and IP video will represent 82 percent of all traffic. This increasing demand for highly scalable and efficient distribution of contents requires new alternative solutions for the upcoming Next Generation Internet (NGI), as the existing Internet architecture is becoming inadequate [2]. Information Centric Networking (ICN) is one of the NGI alternatives, which focuses on contents rather than end-points [3]. ICN relies on unique attributes such as location independent naming, in-network caching, name-based routing and built-in security [4].

In ICN architectures, there are new attacks that have appeared in addition to the legacy attacks that may have an impact on ICN traffic. ICN changes the security model from securing the path to securing the content, which is available to all ICN nodes. This paper discusses the security vulnerabilities in ICN architectures and how they affect ICN security services and components. Accordingly, the main objective of this paper is to build solutions that defend against these security vulnerabilities [5], [6].

- This research has been conducted at School of Computing in Queen's University.

ICN attacks can be classified into naming, routing, caching, and miscellaneous attacks. ICN architectures increase attackers control and censorship on information flow and make blocking information much easier for them. In routing related attacks, malicious publishers and subscribers can publish and subscribe for invalid contents or routes. ICN caching is vulnerable to different kinds of attacks that pollute or corrupt the caching system, in addition to the difference between cached and uncached contents that violates ICN privacy. Other attacks are concerned about unauthorized access and changing contents during transmission.

ICN supports in-network caching, which allows any node to cache contents published by any publisher. ICN does not depend on IP addresses and any user can publish or subscribe for contents. Existing security solutions cannot be applied directly to ICN architectures because of these unique ICN attributes.

To the best of our knowledge, this paper presents the first security framework for ICN traffic management. The main objective of this framework is to study ICN traffic to differentiate between legitimate and malicious user behaviors and hence provide appropriate countermeasures. Any ICN security solution must address three main problems. The first is malicious publications and subscriptions that can be done in a distributed way and negatively affect large-scale ICNs. The solution allows valid publications to be available to legitimate users. The second pertains to unauthorized access, which is exacerbated in ICN since content can be cached and accessed from any ICN node. The third is related to violating private information either about contents or users. We outline such framework that includes countermeasures for these three problems. The framework may be integrated within ICN architectures to deliver contents with high availability and securely to legitimate users and to preserve the privacy of ICN users and contents.

The remainder of the paper is organized as follows. Section II discusses ICN attacks with respect to ICN components and security services and new challenges. Section III presents the proposed framework components. Section IV shows our specific solutions as examples for the framework components and presents some of our results. Section V summarizes the paper.

978-1-5386-7518-2/18/$31.00 ©2018 IEEE
DOI 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00027

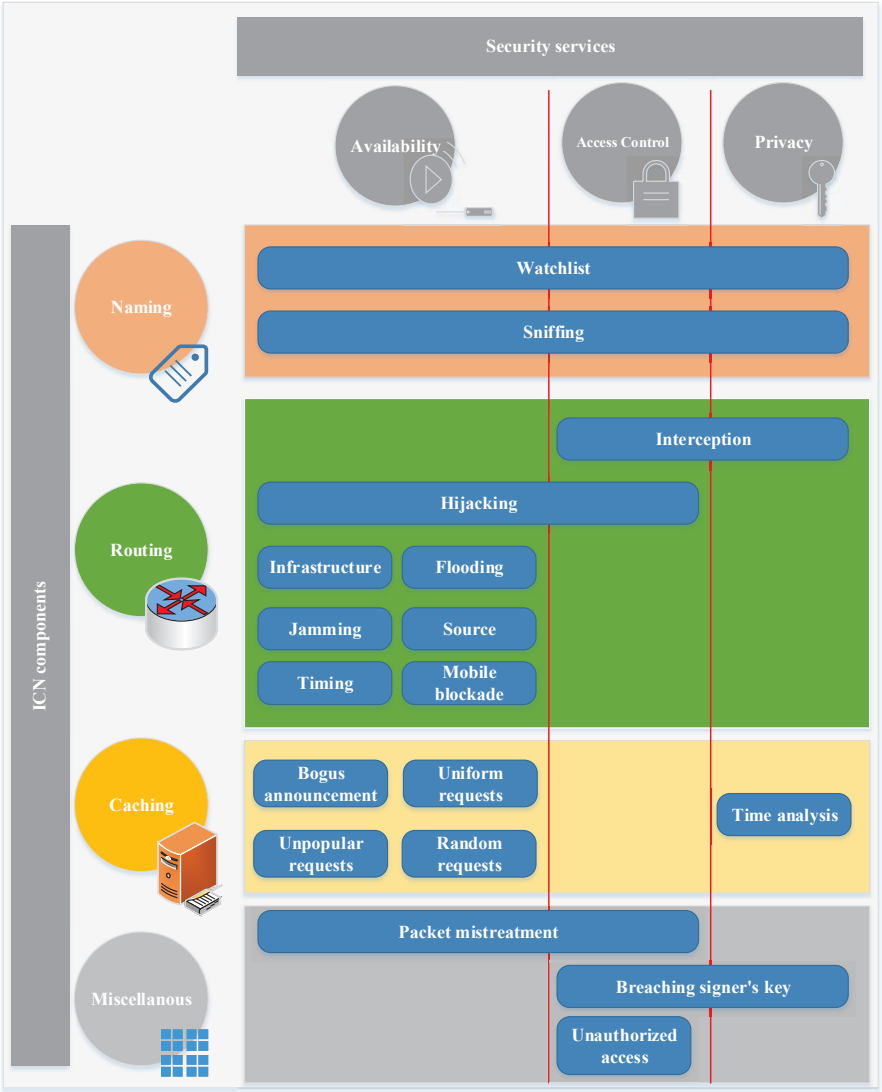


Figure 1: ICN attacks vs. security services: ICN naming, routing, caching, and miscellaneous attacks and their impact on availability, access control, and privacy security services.

II. ICN Attacks

Here, we briefly identify unique attacks to ICN architectures, in addition to other generic attacks that have impact on ICN architectures. 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 a significant impact in other environments. Additionally, many attacks that occur in other environments can also occur in ICN. In an earlier work [2], we presented a comprehensive survey of ICN attacks and their impact. Figure 1 shows the four main attack categories with respect to security services (availability, access control, and privacy). The figure shows how each attack impacts different security services. For example, interception attack affects access control and privacy, while hijacking attack affects availability and access control.

Naming. Self-certifying naming is the most referenced ICN naming scheme. It consists of a cryptographic hash of the owner's public key and label assigned by the owner. Metadata contains the full public key and digital digest signed by the owner. Naming attacks can be classified into watchlist and sniffing attacks. These attacks allow attackers to censor and filter contents. Attackers can also get private information about content popularities and user interests.

Routing. In ICN, routing techniques can be classified into two approaches: name resolution and name-based routing.

ICN content delivery depends on asynchronous publication and subscription. Routing attacks cause Distributed Denial of Service (DDoS), resource exhaustion, path infiltration, and privacy violation. Attackers publish invalid contents, announce malicious routes, and attract legitimate requests. Also, Attackers send large number of malicious requests for available and unavailable contents targeting single source, infrastructure, and specific nodes. The attacks in this category can be classified into DDoS and spoofing attacks. DDoS can be classified into resource exhaustion and timing attacks. Resource exhaustion can be classified into infrastructure, source, mobile blockade, and flooding attacks. Spoofing attacks can be classified into jamming, hijacking, and interception attacks.

Caching. In-network caching allows any node to cache contents coming from any publisher. Attackers send large number of malicious requests with different request distributions. Caching attacks cause cache pollution, privacy violation, and DDoS. The attacks in this category can be classified into time analysis, bogus announcements, and cache pollution attacks. The cache pollution can be classified into uniform, random, and unpopular request attacks.

Miscellaneous. Attackers try to get restricted-access contents. Also, attackers try to break signer's key and behave as legitimate publishers. Additionally, Attackers try to modify, delete, or replay contents. In-network caching attribute maximizes these types of attacks because contents can be accessed from many locations.

Challenges

There is no comprehensive security framework that address the existing main ICN challenges, which can be summarized in the following points:

c1. Attackers send a large number of malicious requests for available and unavailable contents.
c2. Attackers announce malicious routes and send invalid contents.
c3. Attackers send various request patterns to force ICN caches to store unpopular contents instead of the popular ones.
c4. Attackers use in-network caching to get restricted-access contents, which are available in many distributed locations.
c5. Attackers change or send other contents during transmission.
c6. Attackers monitor content names and subscriber requests to filter, block and record private information about these contents and requests.
c7. Attackers measure the difference between cached and uncahed contents to violate subscribers' privacy and get content popularities.
c8. Attackers break signer's cryptographic keys to behave as legitimate publishers.

III. ICN Security Framework

This section presents the proposed security framework that includes the three basic components: availability, access control, and privacy, as depicted in Figure 2. These three security services are the most vulnerable ones in ICN [2], [7]-[18]. The purpose of the availability component is to ensure that legitimate subscribers are able to access contents when needed. The access control component's goal is to deliver contents securely to legitimate users only. The privacy component aims to preserve the privacy of ICN users and contents. There are some common functions that should be applied in this framework.

Our reference model consists of ICN routers, distributed storage location, and ICN users. ICN routers have routing and caching capabilities. The distributed storage locations are used to store the rating for ICN contents and publishers. ICN users are classified into publishers and subscribers. ICN subscribers can send a subscription message or vote against an invalid content. An attacker can be a malicious subscriber or publisher or both. The impact of these attacks can be amplified if the attackers act in a distributed manner. Attackers who control many end systems can cause DDoS attacks on a large scale ICN.

In designing our framework and proposed solutions, we make the following assumptions:

- Depending on ICN self-certifying naming scheme: Our proposed protocols are based on ICN self-certifying naming scheme, which is a promising technique in ICN. Data Oriented Network Architecture (DONA), Network of Information (NetInf), and Publish Subscribe Internet Technology (PURSUIT) architectures are using this naming scheme. Access control protocol based on self-certifying naming does not need to check ICN content integrity and publisher authenticity because they are verified in this naming scheme.
- Backbone network is secure: For access control protocols, we assume that our protocols will be applied in ICN edge routers because these edge routers are accessible by users. The aim of this assumption is to minimize extra authentication messages. In this case, required authentication messages are needed between ICN users and edge routers.

In the following parts, we write the associated challenge for each function between parentheses. For example, **(c1)** refers to challenge number one.

Sign contents. A publisher signs ICN content so that a subscriber can verify the content authenticity and integrity. (c2, c5)

Verify content authenticity. A subscriber compares between sent and received publisher information to ensure that the content is coming from the intended publisher. (c2, c5)

Verify content integrity. A subscriber compares between received signed hash value and subscriber calculated hash

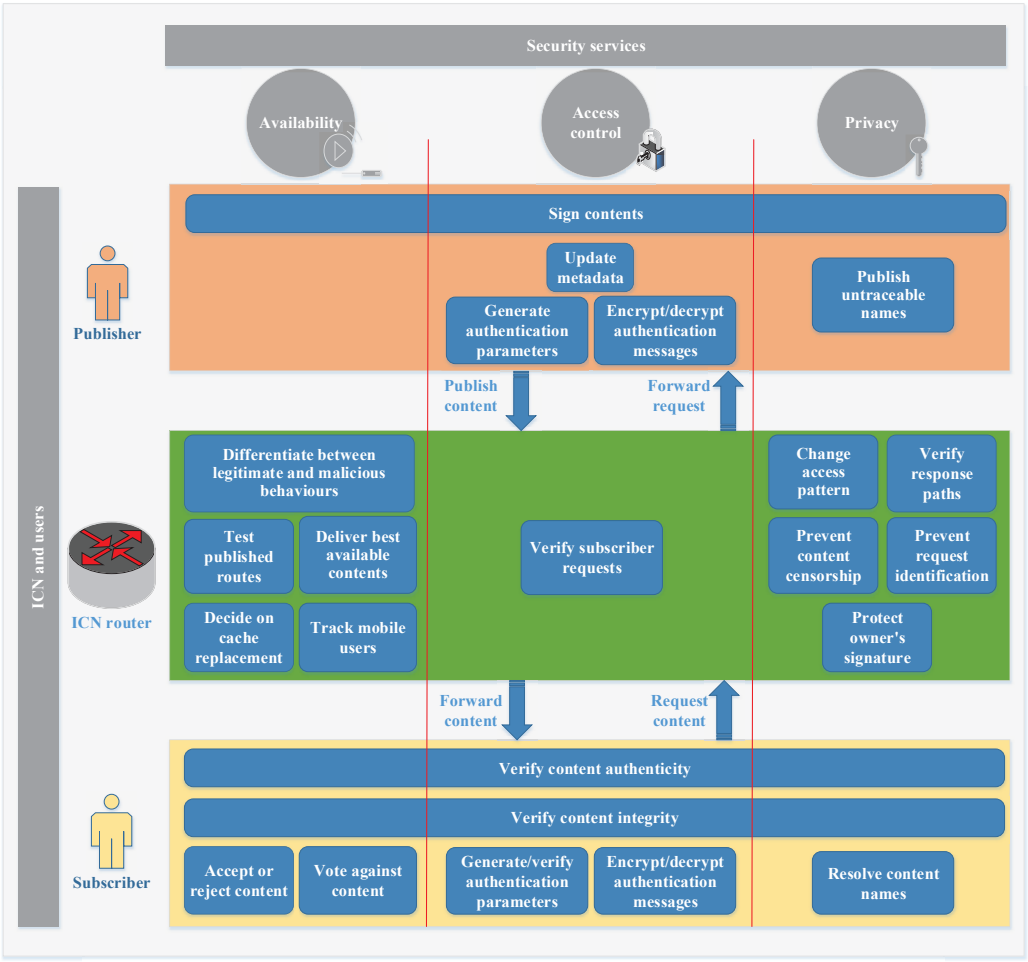


Figure 2: ICN security framework: required security functions at ICN publisher, router, and subscriber to achieve availability, access control, and privacy services.

value to ensure that no one modified the content during transmission. (c2, c5)

In the following subsections, we investigate the three components in detail.

Availability

ICN is an open environment that depends on in-network caching and focuses on contents. These attributes make ICN architectures subject to different types of routing and caching attacks. These types of attacks can be carried out in a large distributed scale to cause DDoS for legitimate users. This component detects and prevents ICN DDoS related attacks to maintain the network availability. Also it preserves the most popular contents in ICN caching in order to deliver contents efficiently [7]–[9]. There are some previous work for ICN security that target DDoS attacks. Afanasyev et al. [11] propose three mitigation strategies to handle flooding-based DDoS attacks through requesting unavailable contents and recommend satisfaction-based pushback mechanism as the best mitigation technique to detect and prevent these attacks in ICN. In [12], Cacheshield uses a shield function that determines whether to cache contents or not at ICN routers to handle random requests for ICN caching. Based on these related work examples and others [2], [7]–[9], the main functions that should be included in this component can be summarized as follows:

Differentiate between legitimate and malicious behaviors. This function evaluates incoming traffic requests and detects legitimate and malicious ones. This function differentiates between legitimate and malicious users based on their behavior on how they send their requests with respect to request rates and request patterns. (c1, c3)

Test published routes. ICN routers use this function to send test messages to the announced routes and decide either these routes are legitimate or malicious based on received

Table I: ICN attacks, framework functions, and security services. The letters in parentheses indicate the function locations. (P): Publisher, (R): ICN router, (S): Subscriber.

ICN Attacks		Framework Function	Security Service
Naming	Watchlist	• Publish untraceable names (P) • Prevent content censorship (R) • Prevent request identification (R) • Resolve content names (S)	Privacy
	Sniffing		
Routing	Interception	• Verify response paths (R)	Privacy
	Hijacking	• Differentiate between legitimate and malicious behaviours (R) • Test published routes (R) • Deliver best available contents (R) • Accept or reject content (S) • Vote against content (S)	Availability
	Infrastructure		
	Source		
	Flooding		
	Jamming		
	Timing		
	Mobile blockade	• Track mobile users (R)	
Caching	Bogus announcements	• Same as routing solutions	
	Time analysis	• Change access pattern (R)	Privacy
	Uniform requests	• Decide on cache replacement (R)	Availability
	Random requests		
	Unpopular requests		
Miscellaneous	Packet mistreatment	• Same as access control solutions	Access Control
	Breaching signer's key	• Protect owner's signature (R)	Privacy
	Unauthorized access	• Sign contents (P) • Update metadata (P) • Generate authentication parameters (P) • Encrypt/decrypt authentication messages (P,S) • Verify subscriber requests (R) • Verify content authenticity (S) • Verify content integrity (S) • Generate/verify authentication parameters (S)	Access Control

responses. ICN routers mark this route as malicious or offer another opportunity to resend subscriber request. (c2)

Deliver best available contents. This function targets to choose the top-ranked content and publisher. This ranking is based on user voting and number of content downloads. This function depends on parameters that should include subscriber request and feedback, publisher behavior, and content popularity. (c2)

Decide on cache replacement. ICN caching replaces least popular content with most popular ones, if the cache is full. ICN caching popularity parameters include subscriber requests and number of requests for each content. (c3)

Track mobile users. This function tracks ICN mobile users in different ICN networks and detects their behaviors, so ICN routers can apply the above functions on these mobile users. (c1, c3)

Accept or reject content. Each subscriber decides to receive or deny the content based on its ranking in terms of content and publisher. (c2, c5)

Vote against content. Subscribers send voting messages against invalid contents to decrease their ranking. As the number of voting messages increased, the voting weight decreased. Vote against content gives a user the chance to provide his or her feedback on the content. (c2, c5)

Access control

Nowadays, in the current Internet architectures, contents are cached at specific servers. This enables network security administrators to deploy their security modules and hence simplifies the access control mechanisms. ICN enables subscribers to access contents from different locations because of the in-network caching attribute. This attribute makes the access control security service in ICN much more complicated than before. Access control component covers ICN confidentiality and integrity.

Fotiou et al. [13] propose a centralized access control mechanism (ACED) that evaluates subscriber requests against access control policies. In this mechanism, there are extra entities such as access control provider and relaying party. Another centralized mechanism for NetInf ICN architecture is presented in [14]. This mechanism uses ID-based cryptographic technique for securing the messages and an extra entity named trusted ticket granting (TTG) for key generation and distribution. Wang et al. [15] propose a decentralized session-based authentication mechanism that can be applied to different ICN architectures. In this mechanism, each ICN content has two names, one is public and the

other is a secure name that is known only by legitimate users. AbdAllah et al. [16] propose a Decentralized Access Control Protocol for ICN (DACPI) that depends on ICN self-certifying naming scheme. DACPI uses RSA public key infrastructure, key exchange using Diffie-Hellman, hashing, and random number generations. We recommend decentralized mechanisms because they do not use extra entities, do not have a single point of failure, and can use less number of authentication messages. According to the aforementioned related work and others [2], [16], the major functions that should exist in this access control component can be summarized as follows:

Update metadata. ICN publisher sends a publication message with the self-certifying content name. The metadata attached with the content is updated with the following information: hashing value of content and random numbers, secret information and cryptographic system public parameter. Cryptographic system encryption and decryption achieve messages confidentiality, while shared secret key, hashing technique, self-certifying naming achieve contents authenticity and integrity. (c4, c5)

Generate or verify authentication parameters. This function calculates and verifies the required authentication parameters at publisher and subscriber sides. (c4, c5)

Encrypt and decrypt authentication messages. Messages are encrypted using receiver's public key and then using sender's private key to achieve authenticity and confidentiality. (c4, c5)

Verify subscriber requests. ICN routers verify subscriber requests be comparing subscriber hashing value with attached content hash value. (c4)

Privacy

The privacy component handles naming, interception, and time analysis attacks. An attacker main goals are to censor contents and know their popularities. This component prevents attackers from knowing content popularities and private information about ICN users. In [17], authors present malicious access privacy issues based on timing analysis attacks and related countermeasures. The time difference can be used as an indicator, if the subscriber has requested this content before or not. Wood et al. [18] personalize ICN cached contents to each ICN legitimate user by proposing encryption-based technique. The essential functions that should be included in this component can be summarized as follows:

Publish untraceable names. Publishers use this function to publish names that cannot be tracked or expected by attackers such as self-certifying naming scheme. (c6)

Change access pattern. The purpose of this function is to prevent an attacker from differentiating between cached and uncached contents. ICN routers can respond with random delays or generate cache misses. ICN routers reply with delays close to the original roundtrip times. (c7)

Verify response paths. An attacker needs extra time to censor and redirect request through certain paths. ICN routers calculate response time and if it exceeds certain threshold, ICN routers neglect these routes. (c2, c6)

Prevent content censorship. This function generates dynamic mapping between actual content name and the submitted one from the subscriber. (c6)

Prevent request identification. This function removes any identification, if exists, so an attacker cannot track who requested what. (c6, c7)

Protect owner's signature. This function protects owner's signature from cryptanalysts. (c8)

Resolve content names. As a part of the framework, this function enables a subscriber to generate the correct name for the intended content. (c6)

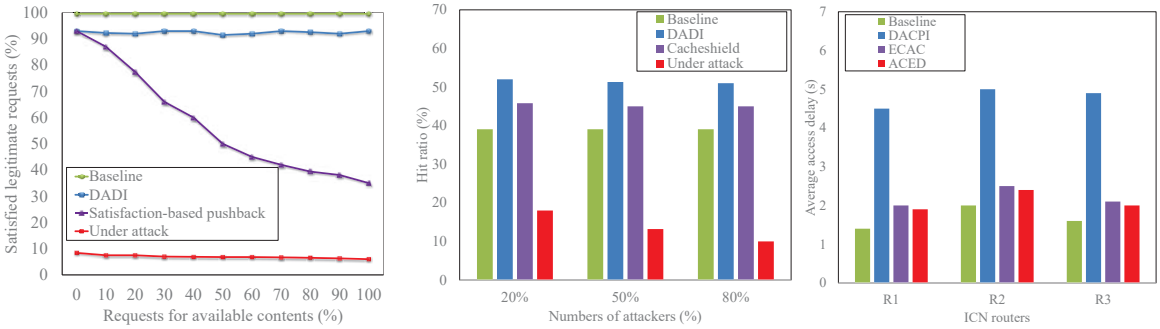
Table I presents and summarizes the relations between ICN attacks, framework functions, and security services.

IV. Some specific solutions

This section shows how the framework can be implemented by discussing some of our proposed solutions for the framework components. We applied the proposed framework using a popular ICN simulator named ndnSIM [20]. We build our experiments using backbone AT&T network, which is an Internet-like architecture. In our experiments, the network consists of 150 subscribers, 10 publishers and more than 40 routers. In our work, we use many network scenarios to test our proposed solutions. We change subscriber request rates, subscribers request available and unavailable, popular and unpopular contents with different percentages. ICN cache sizes are also changed.

A rate-based approach for availability. The solution is implemented in ICN routers based on threshold value calculations and Request Satisfaction Ratio (RSR). The solution consists of detection and prevention phases. In the detection phase, ICN routers are able to differentiate between legitimate and malicious request. In the prevention phase, ICN routers apply appropriate actions based on attack cases. We use other parameters such as request rate, rating for contents, rating for publishers, and rating for cached content, which dependent on the RSR. RSR can be calculated by the number of satisfied requests per user with respect to the outgoing requests from this user. Request rate represents the number of outgoing requests per second for each user. Cache hit ratio indicates the number of cache hits per user with respect to the outgoing requests from this user. Rating for contents indicates the ranking method for ICN contents to select the best available content. Rating for publishers represents the ranking technique for ICN publishers to select the most trusted publisher.

A decentralized approach for access control. We propose a decentralized Elliptic Curve based Access Control (ECAC) protocol. ECAC does not require extra entities or architecture modifications like the centralized mechanisms



(a) Routing (b) Caching (c) Access control

Figure 3: Some of our solution results: (a) percentage of satisfied legitimate requests when attackers send malicious requests for available and unavailable contents, (b) percentage of cache hit ratio when attackers send malicious uniform distribution requests, (c) ICN average request access time delay at three edge routers under different ratios for attackers to legitimate users when 80% attackers exist with cache size = 1000 entry and request rate = 100 req/sec.

or content modifications similar to the encryption-based techniques. Elliptic Curve (EC) has two main advantages. EC can achieve encryption and decryption goal and key exchange goal. Additionally, EC reduces processing overhead because it can offer equal security for a smaller key size compared to the well-known RSA technique [7]. ECAC uses fewer public messages for access control purposes than existing solutions. A publisher sends a message with the content name, hashing value, secret information, and public parameters. A subscriber sends an encrypted message with the content name that achieves both authenticity and confidentiality, and ICN forwards the request to the responsible publisher. Then the publisher also achieves both authenticity and confidentiality by replying with an encrypted message that includes a nonce and public parameters to the subscriber. The subscriber afterwards sends a request with the content name, hashing value, and public parameters to ICN nodes. ICN routers compare between hash values of the received publication and subscriber one. Finally the subscriber also evaluates the content and secret information to be sure that everything is correct.

A pseudonymity-based naming approach for privacy. In this approach, publishers send publication messages with different pseudonymity names. Subscribers send subscription messages for these names. Legitimate Subscribers can retrieve content names easily, while attackers cannot form actual content names without knowing security parameters. ICN routers sends random delays for cached contents and discard routing paths that take longer times. Each ICN router records round trip times for cached contents. In case of attack detection, the ICN edge router connected to the requested interface responds with random delays close to the original round trip times. Also, each ICN router sends an alert message to its attacked users. We detect the attacked users by counting and grouping the common requests between an attacker and each proximate user.

Results

We show some results of our solutions for routing, caching, and unauthorized access, as depicted in Figure 3. Defending Against DDoS attacks in ICN (DADI) is our solution for routing and caching attacks and ECAC is ours for unauthorized access attacks. We used the following performance metrics:

Satisfied legitimate requests. The number of satisfied requests with respect to outgoing requests for legitimate users.

Cache hit ratio. The number of cache hits with respect to the number of outgoing requests.

Request access time delay. It represents the delay between the first interest sent and the data packet received.

For DADI solution, we compare our results with the leading solutions in each category. For publisher side DDoS attacks, our results are compared with the needle in a haystack solution [19]. We compare subscriber side routing related DDoS attacks with the satisfaction-based pushback mechanism [11]. Caching related DDoS attacks are compared with respect to the CacheShield scheme [12]. Our solutions achieve results close to the baseline in some attack scenarios.

For ECAC solution, the experimental results show that the three access control mechanisms increase request access time delay in all cases because of the extra time needed for enforcing access control in ICN. This extra time is coming from either the exchange of access control messages between different entities as in ACED [13] or applying the cryptographic techniques as in ECAC and DACPI [16]. ECAC and ACED achieve similar results in all cases and outperform DACPI. The reason behind these almost similar results between ECAC and ACED comes from the difference between the number of messages required for access control. Although in ACED, there is no encryption and decryption

as in ECAC, the extra messages and exchange of these messages between the extra entities in ACED minimize the time difference between the two protocols. As the cache size increases, request access time delay for all cases and the difference between the three access control protocols and baseline decrease. It happens because the number of cache content evictions decreases as the cache size increases, and hence routers can use their local copies instead of sending requests to the original sources.

V. Conclusion

Information Centric Networking (ICN) is one of the proposed alternatives for the Next Generation Internet (NGI). ICN comes with new challenges and requires new solutions. ICN attacks include threats to naming, routing, caching, and miscellaneous security attacks. We propose a security framework to manage ICN traffic to detect, prevent, and respond to such attacks. The framework contains availability, access control, and privacy components and can be integrated within ICN architectures.

We believe that ICN will be incrementally deployed with non-ICN architectures. The future work stemming from this paper is to implement an interface to connect ICN with non-ICN architectures. This interface should include the appropriate functions and parameters that allow contents to be transferred securely between different types of networks.

Acknowledgment

This work is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Canada Research Chairs (CRC) program.

References

[1] Cisco visual networking index: forecast and methodology, 2015-2020, June 2016.

[2] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking", *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, 2015, pp. 1441-1454.

[3] Md. F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, and B. Mathieu, "A survey of naming and routing in information-centric networks", *IEEE Communications Magazine*, vol. 49, no. 12, 2012, pp. 44-53.

[4] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking", *IEEE Communications Magazine*, vol. 49, no. 7, 2012, pp. 26-36.

[5] F. Almeida and J. Loureno, "Information centric networks-design issues, principles and approaches", *Int. Journal of Latest Trends in Computing*, vol. 3, no. 3, 2012, pp. 58-66.

[6] M. Vahlenkamp, M. Whlisch, and T. C. Schmidt, "Backscatter from the data plane - threats to stability and security in information-centric networking", *Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 57, no. 16, November 2013, pp. 3192-3206.

[7] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, "Countermeasures for mitigating ICN routing related DDoS attacks", *The 10th International Conference on Security and Privacy in Communication Networks (Securecomm14)*, Beijing, China, 2014, pp. 84-92.

[8] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, "Detection and prevention of malicious requests in ICN routing and caching", *The 13th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC-2015)*, Liverpool, UK, 2015, pp. 1741-1748.

[9] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, "DADI: Defending against distributed denial of service in information-centric networking routing and caching", *Wiley Journal of Security and Privacy*, January 2018, e16, DOI: 10.1002/spy2.16.

[10] W. Stallings, "Cryptography and network security: principles and practice", Sixth Edition, Prentice Hall, 2013.

[11] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking", *IFIP Networking Conference*, 2013, pp. 1-9.

[12] M. Xie, I. Widjaja, and H. Wang, "Enhancing cache robustness for content-centric networking", *IEEE Infocom*, Orlando, FL, 2012, pp. 2426-2434.

[13] N. Fotiou, G. F. Marias, and G. C. Polyzos, "Access control enforcement delegation for information-centric networking architectures", *The Second Edition of the ICN Workshop on Information-Centric Networking*, ACM, 2012, pp. 85-90.

[14] M. Aiash and J. Loo, "An integrated authentication and authorization approach for the network of information architecture", *Journal of Network and Computer Applications*, vol. 50, 2014, pp. 73-79.

[15] Y. Wang, M. Xu, Z. Feng, Q. Li, and Q. Li, "Session-based access control in information-centric networks: design and analyses", *IEEE Performance Computing and Communications Conf. (IPCCC)*, Austin, TX, 2014, pp. 1-8.

[16] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, "DACPI: A decentralized access control protocol for information centric networking", *IEEE Symposium on Communication and Information System Security (ICC '16)*, Kuala Lumpur, Malaysia, 2016, DOI: 10.1109/ICC.2016.7511198.

[17] A. Mohaisen, H. Mekky, X. Zhang, H. Xie, and Y. Kim, "Timing attacks on access privacy in information centric networks and countermeasures", *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, 2015, pp. 675-687.

[18] C. A. Wood, and E. Uzun, "Flexible end-to-end content security in CCN", *IEEE 11th Conference on Consumer Communications and Networking (IEEE CCNC)*, Las Vegas, NV, 2014, pp. 858-865.

[19] C. Ghali, G. Tsudik, and E. Uzun, "Needle in a haystack: mitigating content poisoning in named-data networking", *SENT'14*, San Diago, CA, USA, 2014.

[20] A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM: NDN simulator for NS-3", Technical Report NDN-0005, 2012.