

Security Aspects of the Information Centric Networks Model

Amjad Mahfouth

*Computer Information System
Al Quds Open Univeristy
Tulkarm,00970,Palestine*

amahfouth99@gmail.com

Abstract

With development of internet and the enormous growth of contents over networks, that motivated the researchers to proposed new paradigm model called Information Centric Networks ICN , the most features of ICN model is based on the content itself, instead, of the server located the contents over internet. This new model has a lot of challenges such as, mobility of contents, naming, replications, caching, communications, and the security issue to secure the contents, customer, and providers. In this paper we will focus on ICN Model and propose solutions of security to protect the network elements, since the security is based on the packet itself rather than the host-centric.

Keywords: ICN, Denial of Service, Encryption, Digital Signature.

1. INTRODUCTION

The enormous growth of information's, resources, contents over internet and networks, increased demands of the content over internet, translation of contents between different networks, and the complexity of the networks and telecommunication system, that's motivated the researchers to explore a new network paradigm called Information Centric Networks (ICNs), in order to adaptive the growth and complexity of contents' and networks over internet. The most features of Information Centric Networks are the availability and mobility a lot of services to customers and users were offered by different providers and operators. According to [1] statistics, In 2011, mobile traffic rose to 144% than previous year, the annual growth of consumer mobile traffic from 2011 to 2016 is expected 83%, while the global mobile data volume is expected to be 10.8 Exabyte per month in 2016. That's an evidence of increase demand of information from side, and growth of the risks on the contents over internet from other side. Therefore the challenges of security, mobility of contents in Information Centric Networks Models are very complex with the complexity of networks technologies. The applications and services were offered to customers have own authenticity method and use different credentials, reliable and easy-to-use methods are needed to support the new paradigm.

The rest of paper is organized as follow: in section 2, we present and discuss the problem statement of the paper, section 3, describe and present the ICN models with their research projects and its features and challenges, section 3, "security issue" in this section we will discuss and propose new security solutions to protect the contents over network. In last in section 4, we prepare the conclusion and summarize the most features and challenges of ICN model and finally we ask several question related to the security model and its features.

2. PROBLEM STATEMENT

With development of Internet, development of business work over internet and increased the web application based on internet, that's lead to customer eyes to look at internet as major of their business, socials , entertainment , news, searches and a lot of their several interests. The huge capacity of in formations, networks, Telecommunication, translation of information between customers and providers, between different networks over internet , that exerts more challenges to the existing internet architecture, especially, in the appearance of the complexity and the

creativity of Next generation Networks and the appearance of Intelligent devices and Intelligent home, all of the these challenges and the future development of applications , that leads to re-think with existing architecture and explore new paradigm architecture organize the contents over internet and keep its availability for customers. Through dynamic method that achieving the efficiency of contents over internet compared with the existing internet architecture, since the users are interested with availability of contents rather than the contents where resident in networks. The new paradigm called Information Centric Networks (ICNs).

The idea behind of Information Centric Networks approach are modeled using on getting the actual contents instead of host centric architecture approach, which means, the ICN model does not focus on the location of contents, in which server located, and server hosted as the existing architecture. Many of researches projects are modeled on Information Content Networks such as: [2]-[6] most of these researches have been described the Information Centric Information from side and underlying the problems and the solutions of ICN architecture from other side, since every architecture or paradigm have a lot of challenges such as, problems, description of implementation technique on the architecture ,and its hierarchy structure. The ICN architecture is in structure and discussion stage, so a lot of proposed solutions are modeled to describe the ICN architecture with it features.

In this paper we will discuss the Information Centric Networks features, challenges, problems and the security technique on the ICN networks to protect the customers, contents and providers over internet.

3. THE INFORMATION CENTRIC NETWORK APPROACH

The increasing demand [6] for highly scalable and efficient distribution of contents over internet has motivated to develop new network called information-centric networks (ICN), which is based on named data objects.

In current architecture networks approach are host-centric which require contents locations in order to get the contents, also the network communication is based on name host, for example, web servers, PCs, laptop, handset devices and other devices. While in the ICN architecture the users get the contents regardless of the host- centric or the server located the contents, this mobility allows the users to share their contents and data anywhere and anytime. In addition the common goal of ICN in [7] is to achieve efficient and reliable distribution of contents by providing general platform for communication services that are today available in dedicated system such as peer-to-peer(p2p) overlays and proprietary content distribution networks.

The presented ICN architecture explore new challenges features based its structure and its architecture, such as supporting of mobility agent of content , caching, replications, communications, names of data contents and security challenges of model. For each of those features, we can propose a new methodology for thesis in order to classify, checks the optimality, describe the techniques and its architectures, determine the work base, and finally the relation between others features in the network model. Since all of those features were analyzed, and proposed solutions and techniques regards with their details and point of views on project researches which proposed in [2]-[6].

In this paper we will focus on the methodology of security techniques on the model in order to protect the contents over its mobility, caching, replications, and communications between the users and providers.

There a lot of projects were studies and proposed improved solution of ICN network such as [7]:

- TRIAD project (www-dsg.stanford.edu/triad/) [2].
- Data-Oriented Network Architecture (DONA) [3].

- Content-Centric Networking (CCN) [5], currently in the Named Data Networking (NDN) project (www.named-data.org)
- Publish-Subscribe Internet Routing Paradigm (PSIRP) [4], now in the Publish-Subscribe Internet Technology (PURSUIT) project (www.fp7-pursuit.eu)
- Network of Information (NetInf) from the Design for the Future Internet (4WARD) project [6], currently in the Scalable and Adaptive Internet Solutions (SAIL) project (www.sail-project.eu)

While of these projects approaches were different from each others with respect to their details, analysis and the techniques of routing name, caching, request/receive and publish the contents and the its procedure algorithm, mobility and security in the ICN Models, they share many assumption, objectives and architectural specifications. The aim is to develop a network architecture that is better for efficiently accessing and distributing content and that is better cope with disconnections, disruptions effects in the communication service.

4. CONTENT SECURITY MODEL

Since the ICN approaches [8] resulted in content arriving from networks elements other than the locating server, the security model cannot be based on where the packet come from or locating server, instead, ICN design must secure the content rather than path, as suggested in [9][10] and else.

The ICN papers are promising for better security due to the use of digital signatures and securing the packet itself. To ensure the confidently, security of packet are self certifying, packet are authenticated using digital signature, also securing the communications lines between users and providers, and providing encryption/decryption in each packet to secure the packet and provide the confidently. The customers who request the resources or the contents must know the name of contents, in addition the customer must know the contents providers public key, so that he can verify the originality and integrity of content. Therefore the ICN model itself must bind the objects name with its public key of content providers'. To falsify the contents an attacker must register with the ICN system, in result, it mitigated the denial of service attack against the contents due to content-centric flow of traffic rather than the host-centric. Naming contents over ICN model explode the directions of naming object through DNS names as suggested in [11][12], the first naming uses hierarchical human-readable-names, the second naming systems uses self-certifying names, which is un readable by human, the key is bound to the name itself, so the users must use other techniques to determine the name of contents through search engine, or personal provider.

Resources which are requested using the interest packet must have permission or know the key to get validate. Therefore denial of services DoS attacks against resources and providers is mitigated due to packet flow of traffic.

5. CONCLUSION

In this paper we discussed and analyzed the ICN Model approach, also we explained the reasons that motivated the researcher to establish and create the model due to the enormous growth of contents over internet, and achieving the availability, mobility of contents and providing more security strategy to protect the contents, users and consumer of ICN model rather than host-centric. In addition we proposed the most features and challenges in ICN models likes, naming, routing, mobility, caching and security of contents over ICN Model, and we browsing most the researches project, that studies and proposed a lot of different solutions and techniques on ICN model, regards their analysis, point of views, and their experiments techniques. Finally we proposed solution techniques on security models to protect the ICN models regards with its components like, contents, providers, operators, customers, and its features. In addition of the authenticity of contents itself, generating the public key, naming of request model, and the encryption in the content itself, and providing secure communication between source and destination.

Since the ICN model is very young and proposed solutions are insufficient and incompatible. We can ask some of questions, we can trust of security model which presented in this paper to secure the ICN model or not, also does the encryption/decryption need more complex computation, does that effect on the efficiency, availability, and traffic packet in ICN model. Is the system reliable or not. Also we can ask others questions on ICN model features about routing, caching and naming, does they satisfy the efficiency, privacy, keep availability of system and scalability. We can answer on all of these questions in next future researches.

6. REFERENCES

- [1] CiscoSystems. (2011). Cisco Report for IP Growth for 2011-2016. Internet Report, 1, 3.
- [2] Cheriton, D. R., & Gritter, M. (2000). TRIAD: A new next-generation Internet architecture. Retrieved from Available on : <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.33.5878>.
- [3] Koponen, T., Chawla, M., Chun, B.G., Ermolinskiy, A., Kim, K. H., Shenker, S., & Stoica, I. (2007). A data-oriented (and beyond) network architecture. SIGCOMM Comput. Commun. Rev., 37(4), 181–192. doi:10.1145/1282427.1282402.
- [4] Dimitrov, V., & Koptchev, V. (2010). PSIRP project – publish-subscribe internet routing paradigm: new ideas for future internet. In Proceedings of the 11th International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing on International Conference on Computer Systems and Technologies (pp. 167–171). New York, NY, USA: ACM. doi:10.1145/1839379.1839409.
- [5] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., & Braynard, R. L. (2009). Networking named content. In Proceedings of the 5th international conference on Emerging networking experiments and technologies (pp. 1–12). New York, NY, USA: ACM. doi:10.1145/1658939.1658941.
- [6] B. Ahlgren et al., “Second NetInf Architecture Description,” 4WARD EU FP7 Project, Deliverable D-6.2 v2.0, Apr. 2010, FP7-ICT-2007-1-216041- 4WARD / D-6.2, <http://www.4ward-project.eu/>.
- [7] Bengt Ahlgren, Christian Dannewitz, Claudio Imbrenda, Dirk Kutscher, and Börje Ohlman, A Survey of Information-Centric Networking. 0163-6804/12/, 2012 IEEE IEEE Communications Magazine. July 2012.
- [8] Ali Ghodsi, Teemu Koponen, Barath Raghavan, Scott Shenker, Ankit Singla, Janes Wilcox, Information-Centric Networking. Seeing the Forest for the Trees, Cambridge, MA,USA. copyright 2022, ACM 978-1-4503-1059-8/11/11, 2011.
- [9] M. Walfish, H. Balakrishnan, and S. Shenker. Untangling the Web from DNS. In Proc. of NSDI, 2004.
- [10] D. Wendlandt, I. Avramopoulos, D. Andersen, and J. Rexford. Don't Secure Routing Protocols, Secure Data Delivery. In Proc. of HotNets, 2006.
- [11] A. Ghodsi, T. Koponen, J. Rajahalme, P. Sarolahti, and S. Shenker. Naming in Content-Oriented Architectures. In Proc of SIGCOMM, Workshop on ICN, 2011.
- [12] D. Smetters and V. Jacobson. Securing Network Content. Technical report, PARC, October 2009.