A Perspective Towards NCIFA and CIFA in Named-Data Networking Architecture

Ren-Ting Lee, Yu-Beng Leau, Yong-Jin Park and Joe H. Obit

Faculty of Computing and Informatics, Universiti Malaysia Sabah, Jalan UMS,
Kota Kinabalu, Malaysia
LRT@JOSHLRT.COM | lybeng@ums.edu.my
yjp@ieee.org | joehenryobit@gmail.com

Abstract. Named-Data Networking (NDN) is the most promising architecture in the future Internet. NDN ensure high availability of contents and security of the data packet. However, it may disturb the stability and security in NDN routing such as Interest Flooding Attack (IFA). There are many existing detection and mitigation technique about IFA which labelled a non-collusive type of routing threats where it causes the PIT resources to exhausted and legitimate request could not perform in communication. Unfortunately, all the existing countermeasure mechanism could not defend the Collusive Interest Flooding Attack (CIFA). The attacks initiated with a satisfying interest and malicious data producer will reply to the corresponding request before the expiry of existing PIT entries in NDN router along the path. CIFA is classified as low rate intermittent attack which is very difficult in distinguish with legitimate requests. Thus, CIFA is more vulnerable and threatens than previous NCIFA. Moreover, there is no benchmark datasets or any public datasets to perform further experiments on detecting CIFA. Thus, there is a need to produce reliable datasets for future investigation in detection or mitigation relevant attacks in NDN.

Keywords: Named-Data Networking, Interest Flooding Attack, Non-Collusive, Collusive Interest Flooding Attack, Collusive, IFA, NCIFA, CIFA, NDN

1 Introduction

1.1 Internet Trending

The world is changing at a fast pace; The Internet had a shift from client-server based application to multiple clients with client application working with a distributed server. The trending of getting something from the internet such as searching over Google, Baidu and Amazon had become the most common things among the netizen. As the traffics and bandwidth is getting larger, the equipment that deploys classified as high-end which will be costly and it is the key for the whole solution in managing requests in data processing [1]. As the number of devices and users had increased tremendously, availability and security of data are taking for concern.

The original version of this chapter was revised: Post-publication corrections have been incorporated. The correction to this chapter is available at https://doi.org/10.1007/978-981-15-0058-9_70

R. Alfred et al. (eds.), *Computational Science and Technology*,
Lecture Notes in Electrical Engineering 603,
https://doi.org/10.1007/978-981-15-0058-9_46

Future Internet architecture as described is an Information-Centric Networking (ICN) could using naming as request as the name is unique at its own, it can be creating at infinite. Besides that, the data content or the packet is secured in a distributed networking with digital signature or certificate [2]. One of the most promising solutions among the ICN is Named-Data Networking (NDN), fully funded by the U.S. National Science Foundation (NSF) under the Future Internet Architecture (FIA) program [3].

The aims are to solve the host-client IP based limitation in parallel to the growth of Internet networking, the increasing number of new devices appeared in both online services and applications especially in the Internet of Things (IoT) related solution [4]. The comparison of both architectures is shown in Fig. 1.

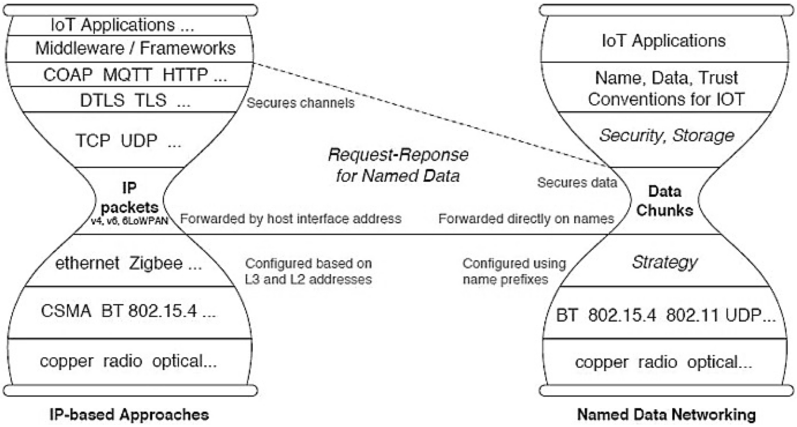

Fig. 1. Internet Architecture of IP-based Approaches versus Named-Data Networking

Fig. 1 shows a comparison between IP-based approaches and Named-Data Networking. The architecture shown in hourglass diagram clearly shown the differences of TCP/IP architecture is using destination address and source address for identification of host and client while NDN using name or data to identify the source rather than channel based communication. NDN is fitted into relevant network operations which traditionally available in IP-based approaches provided within the network layer.

2 Background

2.1 NDN Overview

NDN communication is driven by receivers such as data consumers via the exchange of packets in terms of interest and data [5]. These packets carry an identity which is a name that can be transmitted in a single data packet as shown in Fig. 2. There are 2 types of packets, interest packet is defined by consumer sends it over network and router will forward this name to data producer. Once interest reaches the data requesting node,