Efficient Access Control For NDN based IoT platform

A M. Tech Project Report Submitted
in Partial Fulfillment of the Requirements
for the Degree of

Master of Technology

by

Deshmukh Shubham Madhukar
(194101017)

under the guidance of

Dr. Sukumar Nandi

to the

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
GUWAHATI - 781039, ASSAM

CERTIFICATE

*This is to certify that the work contained in this thesis entitled "**Efficient Access Control For NDN based IoT platform**" is a bonafide work of **Deshmukh Shubham Madhukar** (**Roll No. 194101017**), carried out in the Department of Computer Science and Engineering, Indian Institute of Technology Guwahati under my supervision and that it has not been submitted elsewhere for a degree.*

Supervisor: **Dr. Sukumar Nandi**

Senior Professor,

November, 2020

Department of Computer Science & Engineering,

Indian Institute of Technology Guwahati, Assam.

Acknowledgements

I express my sincere gratitude towards my guide **Dr. Sukumar Nandi**, for giving me this wonderful opportunity to work in this area under his guidance and for his constant support, encouragement and inspiration throughout the project work. I am also very thankful to my Phd scholar Madhurima Buragohain for their motivation and constant support throughout my M.Tech journey.

Contents

List of Figures

Abstract

Information-Centric Networking(ICN) is an emerging networking concept. Named Data Networking (NDN)is an instance of ICN that focuses on what is the content rather than where the host having that content. Internet of Things is today's one of the areas where scalability and security has an important role. Named Data Networking based IoT has gained significance due to the feature like in-network caching. The main objective of the research is a) to analyze why NDN-IoT is better than state-of-art protocols based on TCP/IP as well as other protocols in NDN and, b) propose the effective access control mechanisms for NDN-IoT.

Chapter 1

Introduction

End-to-End is a well-established network architecture. And it is widely used by the people. Mobile devices and the Internet Of Things bring an era where the number of internet users increased drastically. Eventually, it leads to the user requirement of speed, IP address space, etc. As far as speed is concerned, traditional architecture lies on "where is the content" rather than "what is the content". Hence researchers have been focusing on "what is the content" results in faster content retrieval. This new architecture is known as "Content-Centric Networking (CCN)"[6]. Named Data Networking(NDN)[7]is the instance of the CCN.

Traditional IoT[3] has its protocol stack based on TCP/IP. NDN-IoT[10] is an alternative to the existing protocol stack based on Named Data Networking. In-network caching, Reliability, Security are the aspect of NDN motivates the researcher to come up with NDN based IoT protocol. IoT consists of a massive number of things and, failure of the devices due to factors like environment and excessive power is inevitable. Thus adding to the NDN features, automation, and service discovery makes the NDN-IoT implementable.

NDN-IoT is a novel framework. Due to which many researchers are working on various modules like Publish/Subscribe, Access control, Quality of service, etc. In the

paper, we have focused on the efficient access control mechanism in the NDN-IoT as well as its superiority over other protocols.

Chapter 2

Review of Prior Works

In [1] A. Aboodi et al. described the necessity of NDN in IoT[3]. Constraint resources such as fixed memory, limited processing power, low bandwidth impose a heavy burden on the TCP/IP based IoT. Content-based naming and in-network caching made the NDN[7] suitable for such a constraint environment. Such content-based architecture process and communicate data by name without exactly knowing the location of original content producer, simultaneously achieving the security, scalability, and performance. In NDN, valid users can access the data using prefix names. Data validation and verification are performed between the nodes by self-authentication mechanisms. In [9] Shang et al. described how NDN is suitable for IoT by addressing the various IoT challenges.

In [4] Cenk Gündoğran et al. compared the different IoT protocols based on TCP/IP as well as NDN. The comparison was based on factors like transport layer, Pub/Sub mechanisms, Pull, Push, Flow control, and Reliability.

Cenk Gündoğran et al. explained the HoPP [5], a light-weight publish-subscribe scheme based on NDN. Stateful forwarding and in-network caching properties used for energy conversation and robust communication by HoPP.

The comparative study [4] did not include NDN-IoT. Thus our work included the comparative study of NDN-IoT along with the current standard protocol.

Chapter 3

Proposed Work

In the comparison study, We have considered MQTT[2], the state-of-art TCP/IP based IoT protocol, and HoPP[5] lightweight NDN based IoT protocol. NDN based IoT protocols outperform MQTT in the multi-hopped topology[4]. Our comparison based on factors such as pub/sub model, security and Access control, pull/push request, and, Quality of Service, etc. similar to the work in [4]

3.1 Security and Access Control

MQTT provides layer-wise security. At the network layer, it is necessary to have a virtual private network or physically secure network for safe communication between client and broker. At the transport layer, existing TLS and SSL mechanisms are used for encrypting and decrypting communication provided by the existing TCP/IP layer. At the application layer, Client authentication is carried out using protocols such as OAuth or conventional username and password. Unlike MQTT, NDN-IoT and HoPP use self-authenticating mechanisms like a signature. The major drawback of MQTT is that access tokens like a session key are stored on the broker (cloud). It may lead to unauthorized access to stored credentials as well as sensitive data due to bad configuration on the broker's end.

3.2 Publisher-Subscriber Model

Client and broker are the main components of MQTT based on the publish-subscribe model. The client can be a publisher or subscriber but can not be both at the same time. If bi-directional communication is needed then in MQTT, two connection has to be established via a broker. Device instance can act as a publisher whenever it wants to send the data and acts as a subscriber whenever data has to be received. In NDN-IoT and HoPP, a device instance can act as a subscriber and publisher at the same time. Thus, it eliminates the extra connection establishment and hence increases the speed.

3.3 Pull/Push

Push mechanism is used by MQTT[4] that is information is sent at a time for a single connection either from publisher to broker or from broker to subscriber. In contrast to MQTT, HoPP uses a Pull[4] mechanism to get the information. Whereas NDN-IoT uses both pull and push mechanism[10]. Hence NDN-IoT is superior to HoPP and MQTT.

3.4 Quality of Service

MQTT has different QoS levels [2] define the guarantee of delivery. Whereas NDN-IoT and HoPP use reliability and flow control mechanisms of NDN like PCON[8].

	TCP/IP based	NDN based	
	MQTT	HoPP	NDN-IoT
Transport	TCP	NA	NA
Pub/Sub	✓	✓	✓
Push	✓	✗	✓
Pull	✗	✓	✓
Flow Control	✓	✓	✓
Reliability	(Q0,Q1,Q2)	✓	✓

Fig: **Comparison of MQTT, HoPP and NDN-IoT**

Fig. 3.1 Comparison of MQTT, HoPP and NDN-IoT

3.5 Proposed Access Control Mechanism

NDN-IoT is implemented as an NDN-lite framework. The existing implementation uses attribute-based access control[1]. We have proposed access control based on attributes as well as application. Consider the smart home scenario, in the living room, fan and motor, two instances are installed. And the user wants to access the fan and motor. In such a scenario, the role-based access control policy makes two entries in the access control list, one for the fan and the other for the motor. Overhead is introduced due to different entries.This drawback is removed by the policy based on role.

Now consider another scenario of departments on campus. Each professor of the department has different access policies to access the labs according to their profile. In such cases allowing all the resources based on the "professor" as a consumer leads to access to unnecessary resources to all the professors even if it is not needed leads to security issues. Thus only role-based or only attribute-based policy is not sufficient to reduce the overhead while maintaining the security concern.

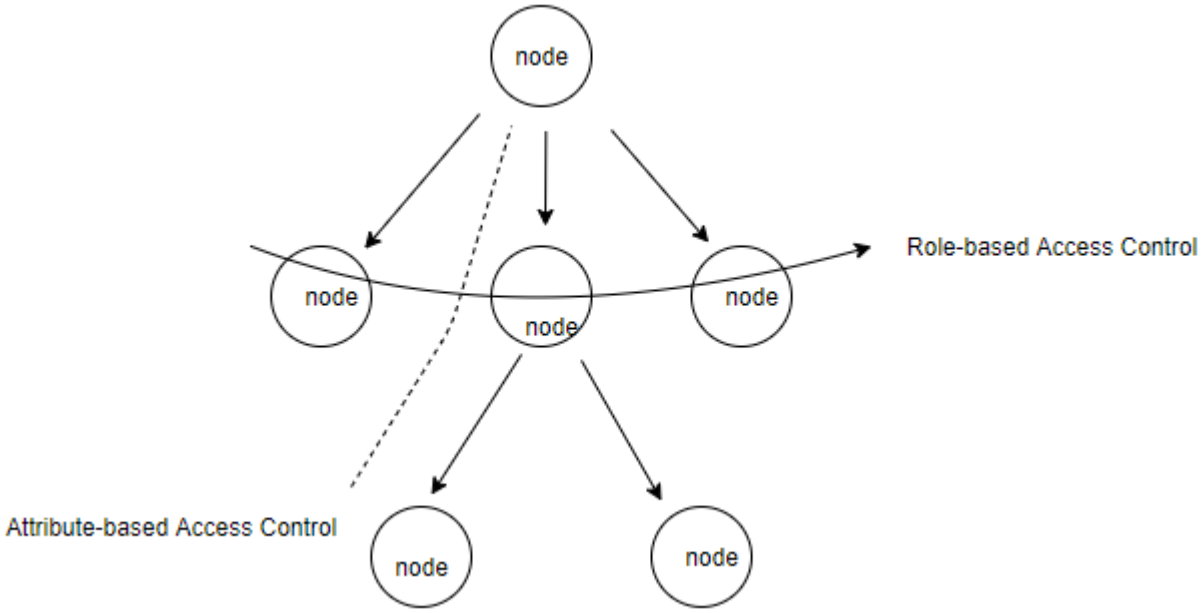

Fig. 3.2 Flow of Access Control Policy

Our proposed policy allows access based on hierarchies. For example, a role-based

access control policy can be applied to the nodes present at the same level. Attribute-based access control policy can be applied to the nodes present at different levels down the hierarchy as shown in Fig. 3.2. Thus it is an efficient access control policy rather than only role-based or only attributes-based.

The corresponding module (Fig. 3.3)[11] in NDN-loT does the service discovery.

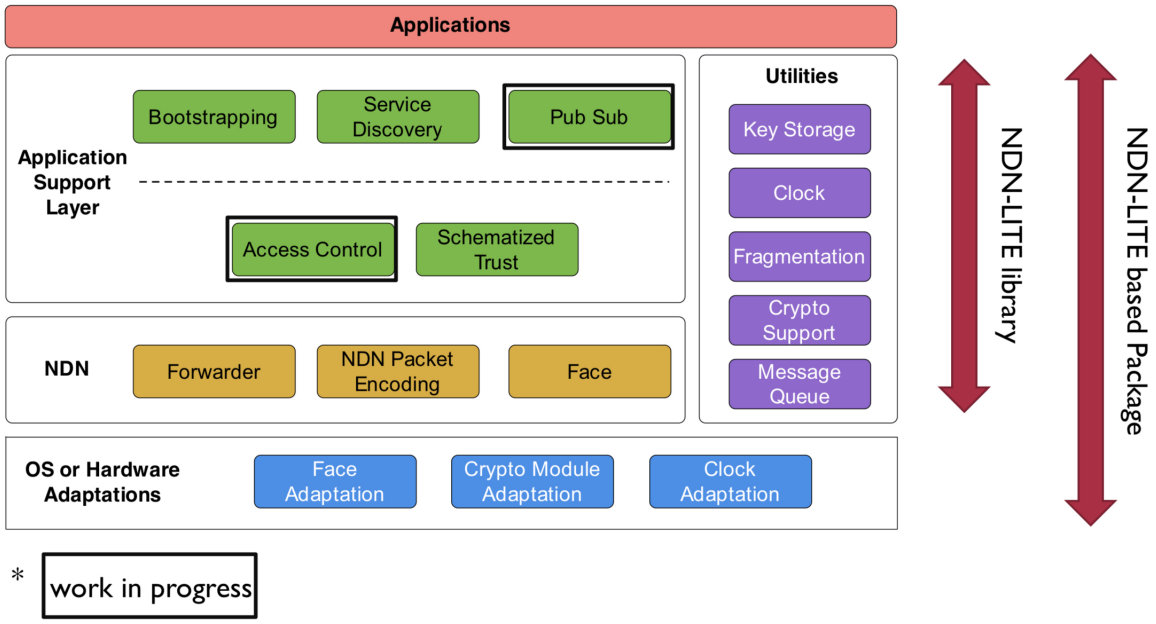

Fig. 3.3 Framework of NDN-Iite (NDN-IoT)

The local controller performs the key-distribution. Due to the local controller, the user has complete control over the data produced and consumed. Thus privacy of data is maintained. The key distribution is shown in fig. 3.4 and Fig. 3.5

The encryption key is obtained for the encryptor to encrypt the content by negotiating with the controller (Fig. 3.4). Encrypter sends the key-request to the controller. The controller sends the Request response data based on the access control policy using the public key of the encryptor. Symmetric Key exchange is performed during the bootstrapping.

Similarly, the decryption key is obtained for the decryptor by negotiating with the controller (Fig. 3.5)

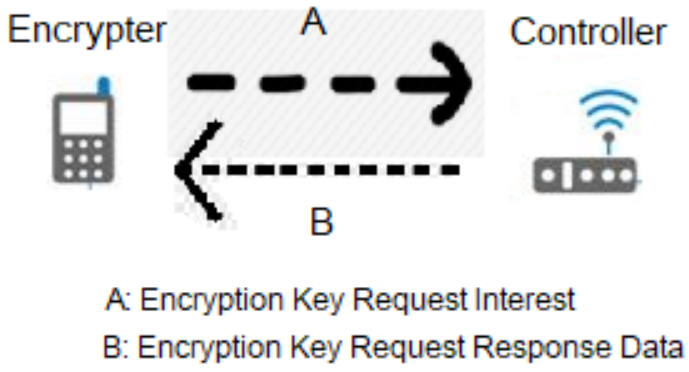

Fig. 3.4 Negotiation Between Encryptor and Controller

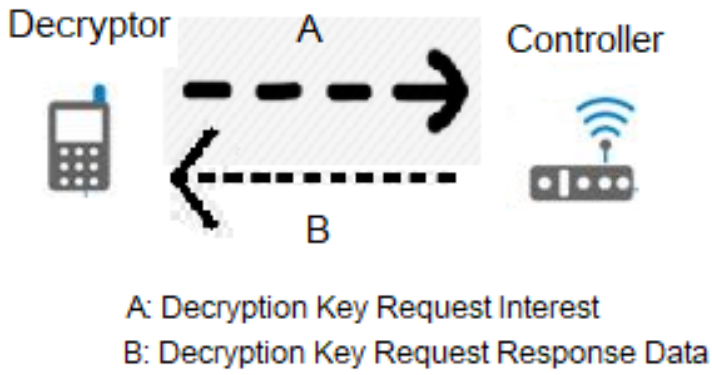

Fig. 3.5 Distribution Between Decryptor and Controller

Data is consumed by sending the content interest from Decryptor and receiving encrypted content Data from the Encryptor (Fig. 3.6). In this way, content is requested and obtained using different access control policies.

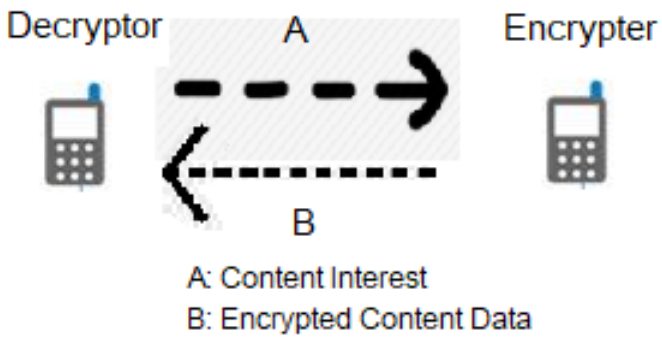

Fig. 3.6 Encrypted Content Data

Chapter 4

Conclusion and Future Work

In this paper, we have compared the MQTT, TCP/IP based IoT protocol, HoPP, and NDN-IoT NDN based IoT protocols. We have observed that NDN-IoT outperforms the HoPP and MQTT. Also, we have proposed the approach to solving the problem of access control only based on attribute or role. The proposed method is based on the hierarchy of the users in a constraint environment such as limited memory, less computing power, and low bandwidth. Our future work involves the implementation of the proposed access control mechanism in NDN-lite.

References

[1] A. Aboodi, T. Wan, and G. Sodhy. Survey on the incorporation of ndn/ccn in iot. *IEEE Access*, 7:71827–71858, 2019.

[2] Andrew Banks and Rahul Gupta. Mqtt version 3.1.1. oasis standard. oasis.

[3] Arindam Giri, Subrata Dutta, Sarmistha Neogy, Keshav Dahal, and Zeeshan Pervez. Internet of things (iot): A survey on architecture, enabling technologies, applications and challenges. In *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, IML '17, New York, NY, USA, 2017. Association for Computing Machinery.

[4] Cenk Gündoğran, Peter Kietzmann, Martine Lenders, Hauke Petersen, Thomas C. Schmidt, and Matthias Wählisch. Ndn, coap, and mqtt: A comparative measurement study in the iot. In *Proceedings of the 5th ACM Conference on Information-Centric Networking*, ICN '18, page 159–171, New York, NY, USA, 2018. Association for Computing Machinery.

[5] C. Gündoğan, P. Kietzmann, T. C. Schmidt, and M. Wählisch. Hopp: Robust and resilient publish-subscribe for an information-centric internet of things. In *2018 IEEE 43rd Conference on Local Computer Networks (LCN)*, pages 331–334, 2018.

[6] Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, and Rebecca L. Braynard. Networking named content. In *Proceedings of the*

5th International Conference on Emerging Networking Experiments and Technologies, CoNEXT '09, page 1–12, New York, NY, USA, 2009. Association for Computing Machinery.

[7] Deborah Estrin Lixia Zhang, James D. Thornton Jeffrey Burke, Van Jacobson, and Diana K. Smetters. Named data networking (ndn) project. Technical report, 2010.

[8] Klaus Schneider, Cheng Yi, Beichuan Zhang, and Lixia Zhang. A practical congestion control scheme for named data networking. In *Proceedings of the 3rd ACM Conference on Information-Centric Networking*, ACM-ICN '16, page 21–30, New York, NY, USA, 2016. Association for Computing Machinery.

[9] W. Shang, A. Bannis, T. Liang, Z. Wang, Y. Yu, A. Afanasyev, J. Thompson, J. Burke, B. Zhang, and L. Zhang. Named data networking of things (invited paper). In *2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 117–128, 2016.

[10] Zhiyi Zhang, Edward Lu, Yanbiao Li, Lixia Zhang, Tianyuan Yu, Davide Pesavento, Junxiao Shi, and Lotfi Benmohamed. Ndnot: A framework for named data network of things. In *Proceedings of the 5th ACM Conference on Information-Centric Networking*, ICN '18, page 200–201, New York, NY, USA, 2018. Association for Computing Machinery.

[11] Tianyuan Yu Edward Lu Xinyu Ma Zhiyi Zhang, Yanbiao L. Ndn-lite architecture.