Poster: Emergency Message Delivery Mechanism in NDN Networks

Toru Hasegawa
Osaka University, Japan
t-hasegawa@ist.osaka-u.ac.jp

Yasutaka Tara
Osaka University, Japan
y-tara@ist.osaka-u.ac.jp

Kai Ryu
Osaka University, Japan
k-ryu@ist.osaka-u.ac.jp

Yuki Koizumi
Osaka University, Japan
ykoizumi@ist.osaka-u.ac.jp

ABSTRACT

ETSs (Emergency Telecommunication Services) in packet networks are promising in terms of resiliency to failures and service delivery to handicapped persons who cannot use voice communications. In this paper, we propose an NDN (Named Data Networking)-based emergency message delivery mechanism for ETS services by leveraging multicasting and ABE (Attribute-Based Encryption) functions. The proposed mechanism not only satisfies the requirements to conventional telephone-based emergency calls, but also provides resiliency to failures.

CCS Concepts

•**Networks** → **Naming and addressing; Network protocol design;** •**Security and privacy** → *Security protocols;*

Keywords

NDN (Named Data Networking); Emergency Call; ABE (Attribute-Based Encryption)

1. INTRODUCTION

Emergency calls in telephone networks have problems inherent to circuit based voice communication such as vulnerability to network fragmentation due to disasters and unavailability for handicapped persons. In order to resolve the problems, we propose *emergency message delivery* in NDN (Named Data Networking) networks, which enables it for us to send an emergency message by using SNS tools. In this paper, we design an NDN-based mechanism to satisfy indispensable requirements to emergency calls in telephone networks. The first requirement is that an emergency message is delivered to an emergency server of the nearest emergency office to an emergency caller. The second requirement is that a location of an emergency caller is securely notified to the server.

We regard that emergency message delivery is similar to IP anycasting, because emergency calls in telephone networks assume a well-known number like 119 and 911. Thus we design an emergency message delivery mechanism as an anycasting service at the naming layer by leveraging multicasting and ABE [3] functions so that an emergency message is delivered to the nearest emergency server among those which have the same well-known name without its location being leaked.

2. REQUIREMENTS

In this section, we identify requirements to emergency message delivery by carefully analyzing those in telephone networks in Japan [2]. We extract the two requirements from those in telephone networks.

(I) An emergency message is delivered to the server of the nearest emergency office like a fire station to an emergency caller.

(II) A location of emergency caller is securely notified to an emergency server.

We need take care of implicit assumptions in telephone networks to satisfy the requirement (II). The word "securely" means that a location of an emergency caller is not leaked to anyone other than the nearest emergency office and that the location is guaranteed by a trusted party like a telecommunication carrier.

3. ARCHITECTURE

A key idea behind the mechanism is that an emergency message is delivered to all emergency servers with an encrypted location of an emergency caller and that the only sever which has the decryption key for the location can decrypt it. COPSS [1] and ABE [3] are used as multicasting and public key encryption mechanisms, respectively.

3.1 Anycasting based on COPSS

Figure 1 shows the anycasting service at the naming layer, which is designed based on COPSS. An intuitive way of naming such a service is using the same number used in telephone networks such as 119 and 911.

A rough sketch of emergency message delivery is as follows: First, the RN(Rendezvous Node) advertises its name (*/Rendezvous*) and the CD (content descriptor) of the service (*/119*) into the name-based routing protocol, wherein the RN and CD work as a rendezvous point and a multicast address of multicasting. In Fig. 1, the routing protocol inserts these two names into the FIBs (Forwarding Information Bases) of all NDN routers. Second, all emergency servers subscribe the CD */119* by sending a subscribe mes-

ICN'16 September 26-28, 2016, Kyoto, Japan

ACM ISBN 978-1-4503-4467-8/16/09.

DOI: http://dx.doi.org/10.1145/2984356.2985234

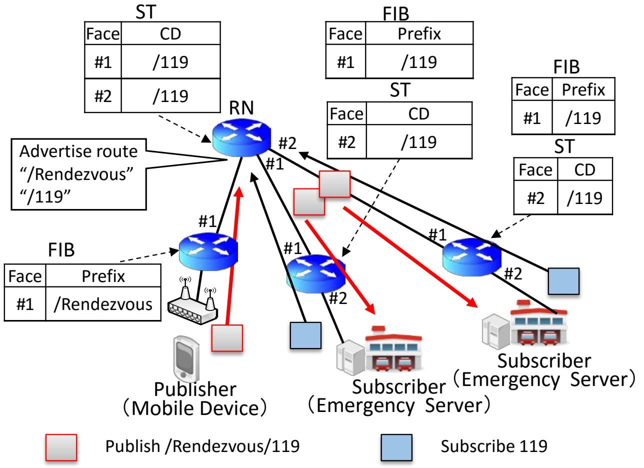

Figure 1: Multicastings by using COPSS

sage with the CD */119*. The subscribe message is forwarded to the RN according to underlying name-based routing. NDN routers which forward such a subscribe message record the CD at the ST (Subscriber Table), which corresponds to a multicasting routing table of IP multicasting. When the RN receives all the subscribe messages, a multicasting tree from the RN to all the emergency servers is created.

Third, an emergency caller sends a publish message with a cypher text of its location to the RN and the name of message is */Rendezvous/119*. The publish message is forwarded via the multicasting tree to all the emergency servers after its name being changed from */Rendezvous/119* to */119*.

3.2 Encryption of Location Using ABE

We adopt ABE to encrypt a location of an emergency caller to prevent the caller from obtaining public keys of all emergency servers in advance. Figure 2 shows how ABE is used to encrypt a location of an emergency caller. First, a master public key is created by a trusted party called a *KGC (Key Generation Center)* and it is delivered to an emergency caller.

Second, the emergency caller uses the master public key to create a public key by specifying attribute values of variables and then encrypts a plain text, i.e., a location, using the created public key. In our architecture, we use x-y coordinates according to Cartesian coordinate system as attributes, which specify a location of an emergency caller as a pair of latitude and longitude values. For example, the location of longitude “135.31" and latitude “34.49" is denoted as “x = 135.31" and “y = 34.49", wherein x and y are attributes.

Third, on the contrary, a Boolean predicate over attributes as a secret key is created by the KGC and the secret key is delivered to an emergency server. For example, the secret key corresponds to the rectangle which the emergency server covers and it is specified by the predicate over x-y coordinate attributes, i.e., $(135.28 < x < 135.33)$ and $(34.46 < y < 34.53)$. The emergency server is able to decrypt a cypher text if attributes of the public key used by encryption satisfy the Boolean predicate over the attributes of the secret key. In Fig. 2, the attributes of “x = 135.31" and “y = 34.49" satisfy the Boolean predicate $(135.28 < x < 135.33)$ and $(34.46 < y < 34.53)$ and thus the emergency server is able to decrypt a cypher text created by the public key. Otherwise, it fails to decrypt the cypher text. This enables it for only the emergency server which is responsible for the area of the emergency caller to decrypt the location.

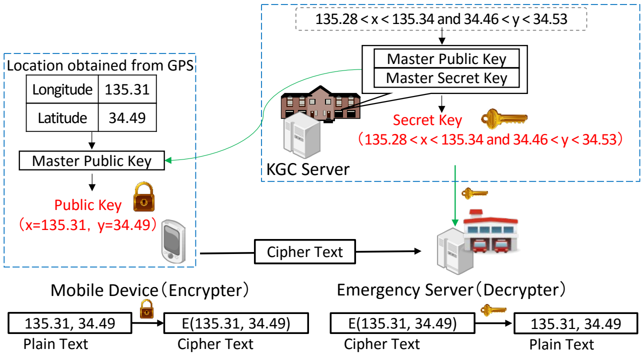

Figure 2: Overview of ABE

4. PRELIMINARY ANALYSIS

An important scalability issue is unnecessary decryption computation at an emergency server because all emergency messages are delivered to all emergency servers. We roughly estimate computation time at an emergency server and shows that such redundant computation rarely matters.

First, we estimate an average interval between emergency calls by analyzing the report of emergency calls in Tokyo. Since the average call number is about 2,923 in one day, the average interval is about 30 seconds in Tokyo. Second, we estimate decryption time of a cypher text based on ABE by uing the public KP-ABE software [3] on the machine (Xeon X5570 2.93GHz). A cipher text (28KB) is made from the text file(49KB). The predicate of the secret key is $(135.28 < x < 135.33)$ and $(34.46 < y < 34.53)$. We measure the decryption time at 100 trials and it is about 0.13 second. This implies that a single PC server is enough to handle all emergency messages at a metropolitan city like Tokyo.

5. CONCLUSION

This paper designs an emergency message delivery mechanism in NDN networks. The contributions of the paper are summarized as below. First, the paper integrates multicasting and ABE so that an emergency message is delivered to the nearest emergency server without leaking information about a location of an emergency caller. Second, adoption of ABE eliminates the need for public key exchanges between all callers and emergency servers. Third, the preliminary analysis shows feasibility of the mechanism.

Acknowledgement

The research leading to these results has received funding from the EU-JAPAN initiative by the EC Horizon 2020 Framework Programme Grant Agreement No. 723014 and NICT under Contract No. 184.

6. REFERENCES

[1] J. Chen, M. Arumaithurai, L. Jiao, X. Fu, and K. Ramakrishnan. Copss: An efficient content oriented publish/subscribe system. In *IEEE/ACM Symposium on ANCS 2011*, pages 99–110, 2011.

[2] Ministry of Internal Affairs and Communications. Functions of Emergency Telecommunication Services. Also available at http://www.soumu.go.jp/menu_seisaku/ictseisaku/net_anzen/hijyo/tuho.html.

[3] Y. Zheng. KP-ABE, Mon Nov 3 19:03:37 2014. Also available at https://github.com/gustybear/kpabe.