Demo:Content-based Push/Pull Message Dissemination for Disaster Message Board

Tomohiko Yagyu
NEC Corporation
Kawasaki, Japan
yagyu@cp.jp.nec.com

Kenichi Nakamura
Panasonic Corporation
Tokyo, Japan
nakamura.kenken@jp.panasonic.com

Tohru Asami
The University of Tokyo
Tokyo, Japan
asami@akg.t.u-tokyo.ac.jp

Kohei Sugiyama, Atsushi Tagami
KDDI R&D Laboratories
Saitama, Japan
{ko-sugiyama, tagami}@kddilabs.jp

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

Mayutan Arumaithurai
University of Goettingen
Goettingen, Germany
mayutan.arumaithurai@cs.uni-goettingen.de

ABSTRACT

Information Centric Networking (ICN) is one of the promising technologies to support reliable communication in the post-disaster network. This demo presents the integrated framework of push and pull type content-based communication, along with proposed enhancements that make it applicable in a disaster scenario. We will demonstrate these features with the help of an example application – disaster message board.

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]: Network Architecture and Design, Network Protocols

Keywords

Information Centric Networking, Fragmented Network, Disaster Message Board, COPSS, Logical interface, IBAS

1. INTRODUCTION

Name-based communication architecture, namely ICN (Information Centric Networking), is useful not only in ordinary cases but also in disaster cases. Aftermath of disaster, existing communication infrastructure such as the Internet and cellular networks will be severely damaged. Because of the fault of BaseStations(BS) and cable cut between BS and backhaul, the infrastructure will be fragmented into portions. We call this partitioned network a fragmented network. The fragmented network comprises of some isolated domains. DataMules(DMs) go round and relay messages among isolated domains. Figure 1 is an example of fragmented network that we assume. In the fragmented network, it is difficult to keep connection with the server. Furthermore, securing the content itself is more feasible than establishing secure connection with the server. Therefore content-based message delivery is more desirable than host-based communication for the service reliability. This demo shows content-based disaster message board in fragmented network. Disaster message board is a bulletin board system used for communication among relatives during disaster[1]. Figure 2 shows the protocol stack of the proposed framework. This framework integrates several achievements[3][4][5][6] in GreenICN project[2] and CCN(Content Centric Networking)[8].

ICN'15, September 30–October 2, 2015, San Francisco, CA, USA.
ACM 978-1-4503-3855-4/15/09.
DOI: http://dx.doi.org/10.1145/2810156.2812609.

2. INTEGRATION OF PUSH AND PULL

In [6], we have demonstrated reliable pull-type communication in the fragmented network. Pull-type communication is useful when a user requests an existing content. However, if a user wants to obtain irregularly generated contents, push-type delivery such as pub/sub is preferable to pull. Push-type communication is also desirable for prompt dissemination of critical information to hundreds of people simultaneously. However in disaster situation, users' devices are often disconnected from the network because of saving their batteries or going outside. Therefore subscribers may fail to receive messages during their absence. When they try to retrieve missed messages, ICN is better architecture than IP network. This is because ICN allows a user to obtain a content by indicating its name without connecting the server. A user can obtain the content from cache in an intermediate node. Therefore integrated framework of push-type and pull-type communication enables reliable and efficient message dissemination in the fragmented network.

COPSS(Content Oriented Publish/Subscribe System)[3] is the name-base pub/sub protocol with Rendezvous Point (RP) node. However, COPSS can not be applied to the fragmented network because 1) intermediate nodes don't cache contents 2) subscribers can't detect missed contents. To retrieve missed messages, first of all, subscribers need to know

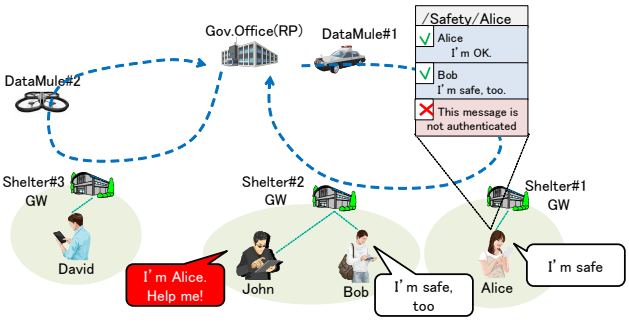

Figure 1: Demo Setup (Disaster Message Board)

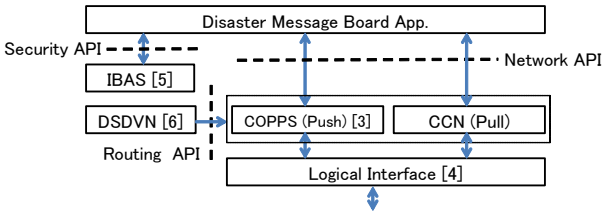

Figure 2: Protocol Stack

whether they have missed some messages or not. We extend RP of COPSS to give a sequence number to each message per topic. A subscriber can detect missed message by the sequence number. Furthermore, every intermediate node is extended to cache the messages and record the latest sequence number for the topics. A subscriber can know the latest sequence number for the topic from the nearest node. If he wants to retrieve the missed message, he pulls it by sending *Interest*. He can quickly obtain the message from the cache in an intermediate node.

3. RELIABLE MESSAGE TRANSMISSION

COPSS relies on a subscription tree rooted at an RP in order to push content from the publishers to the subscribers. In a disaster scenario, wherein there exists fragmented network, such a tree is not straightforward. Therefore, we propose that the isolated domains in fragmented network acts as nodes of the tree and the data-mules behave as logical links that interconnect these domains. Logical Interface(LIF)[4] is the technology to reliably transmit COPSS and CCN messages via intermittent links. LIF stores outgoing messages when the next hop node is disconnected. DSDVN, a routing protocol[6], informs LIF module of the link state. When a new next hop is discovered, LIF module makes a new port correspondent to it. COPSS and CCN send messages to LIF port instead of actual next hop. DSDVN populates FIB entries with LIF ports correspondent to the actual next hops.

4. SENDER AUTHENTICATION

In disaster situation, it is important to authenticate information for preventing false rumors. There are two issues: (1) Trustable servers or certificate authorities on which PKI depends may not be available due to disconnection from the global network. (2) Since bulletin board messages are usually short, the packet overhead for authentication is comparatively burden. Identity-based Aggregated Signature (IBAS)[7] is introduced to solve (1) and (2), which uses public identity such as e-mail address for authentication and reduces the signature size by aggregation. To ensure authenticity of both the message body given by publisher and the sequence number by RP, IBAS aggregates the two signatures required for publisher and RP into one.

5. DEMO SCENARIO

Figure 1 shows the setup of this demonstration. There are three shelters and one government office (Gov.Office) in the disaster stricken area. RP of COPSS is located in Gov.Office. Two DataMules are going round Gov.Office and Shelters. Alice, Bob and David are friends. They subscribe a topic of bulletin board for Alice, named as `/Safety/Alice`, to exchange messages with Alice. When Alice publishes a message with her signature to `/Safety/Alice`, it is forwarded to RP via DataMule. RP puts the sequence number to the message and aggregates signatures of Alice and RP. Then RP sends the message back to subscribers, Alice, Bob and David. Even if Bob is offline at the time, the message is pushed to Shelter GWs. He can get it from the GWs by pull-type retrieval. In addition, they can anthenticate the message with IBAS, even if John sends a fake message with pretending Alice. Demonstration equipments: one laptop runs 10 VMs and wireless connection emulator. Four tablets show the application screens for four users.

6. CONCLUSIONS

We propose content-based framework for relieable, secure and efficient message dissemination in post-disaster fragmented network. In this demo, we show the disaster message board as a reliable service in disaster situation.

7. ACKNOWLEDGMENTS

The work for this paper was partly performed in the FP7/NICT EU-JAPAN GreenICN project.

8. REFERENCES

[1] Requirements for Disaster Relief System, ITU-T Focus Group on Disaster Relief System, Network Resilience and Recovery, Technical Report, May 2014.
[2] http://www.greenicn.org/
[3] J. Chen, M. Arumaithurai, X. Fu, and K. K. Ramakrishnan, "COPSS:An efficient content oriented publish/subscribe system," in Proc.ACM/IEEE ANCS, pp.99-110, Oct. 2011.
[4] K. Sugiyama, A. Tagami , T. Yagyu , T. Hasegawa, M. Arumaithurai, K. K. Ramakrishnan, "Name-based Information Dissemination for Fragmented Networks in Disasters," IEEE ACM COMSNETS 2015, Bangalore, Jan. 2015, Poster session.
[5] B.Namsraijav, Ndn-cxx fork with ibas support. https://github.com/byambajav/ndn-ibas/
[6] T. Yagyu, S. Maeda, "Reliable Contents Retrieval in Fragmented ICNs for Disaster Scenario," ACM ICN2014, pp.193-194, Paris, Sep. 2014, Demo session.
[7] C.Gentry and Z.Ramzan, "Identity-based aggregated signature," In Public Key Cryptgraphy PKC 2006, pp.257-273, Springer, 2006
[8] CCNx implementation, http://www.ccnx.org/