Upgrading Wireless Home Routers as Emergency Cloudlet and Secure DTN Communication Bridge

Christian Meurisch*, The An Binh Nguyen*, Julien Gedeon*, Florian Kohnhäuser*,
Milan Schmittner*, Stefan Niemczyk†, Stefan Wullkotte*, Max Mühlhäuser*
*Technische Universität Darmstadt, Hochschulstraße 10, D-64289 Darmstadt, Germany
Email: {meurisch@tk, nguyen@kom, gedeon@tk, kohnhaeuser@seceng.informatik,
schmittner@seemoo, wullkotte@tk, max@tk}.tu-darmstadt.de
†University of Kassel, Wilhelmshöher Allee 73, D-34121 Kassel, Germany
Email: sni@vs.uni-kassel.de

***Abstract*—Reliable communications are crucial for the success of emergency response and management. However, today's technologies used by rescuers and civilians mainly rely on either centralized or specialized emergency approaches, which reveal individual issues especially in infrastructure-less emergency situations (e.g., blackout). In this paper, we present a customary home router upgraded as self-sustaining emergency device which can ad hoc network with nearby devices (e.g., other upgraded routers, smartphones) using wireless communication technologies. On top of the ad-hoc networking, an upgraded router provides (1) personal computing capacities for low-latency offloading from mobile devices (aka *cloudlet*) using isolated lightweight containers; and (2) store-and-forward delay-tolerant data exchanges to serve as secure communication bridge for cooperation between involved or affected people (e.g., rescuers, civilians). We believe that upgrading ubiquitous routers is a very promising concept for a scalable ad-hoc networking and energy-efficient computing infrastructure in urban emergency situations.**

***Index Terms*—disaster recovery, emergency response, home router, container-based cloudlet, ad-hoc networks, DTN**

I. Motivation

Emergency response and management are challenging tasks, especially if the communication infrastructure - mainly relying on centralized concepts - is impaired or overloaded due to a heavy use as results of crisis situations (e.g., blackout, earthquake). In such crisis cases, today's emergency technologies are limited and rescuers are faced with recovery challenges, e.g., providing alternative reliable communication for enabling cooperation between involved (e.g., rescuers) and affected people (e.g., civilians) [1].

Recent work focuses on ad hoc networking mobile devices (e.g., smartphone) equipped with short-range radios (e.g., WiFi, Bluetooth) for providing decentralized communications in disaster recovery [2]. However, establishing a dense and stable infrastructure is challenging due to their high mobility and short communication range. Since each mobile device also acts as forwarding node, the energy consumption is considerably higher, which has a negative effect on the vital and limited battery life. Moreover, overlying emergency services such as micro-blogging or self-rescue systems use the computational resources of a mobile device to analyze data directly in the network [3], which further runs down the battery.

In this paper, we present ad-hoc networking customary home routers upgraded as self-sustaining stationary emergency devices for (1) computational offloading [4], and (2) bridging communication gaps [3] to reduce the utilization of mobile devices and save valuable energy. We believe that wireless home routers have a great potential as complementary scalable emergency infrastructure due to their dense distribution in urban environments.

II. System Design

We propose upgrading wireless home routers as (1) emergency cloudlet, and (2) DTN communication bridge in ad-hoc network scenarios (cf. Fig. 1). Our previous work already demonstrates that the hardware of such routers is suitable to provide low-latency cloudlet functionalities [5] while the energy-efficiency is high [6]. Using a micro-UPS (uninterruptible power supply), we detect power blackouts and automatically switch to a *self-sustaining emergency mode*. This mode is characterized by creating an isolated *main container* relying on lightweight virtualization techniques with access to the host network interfaces. Within the bootstrap routine, the main container opens a WiFi access point for connecting with unrooted smartphones, and uses another network interface for wireless ad-hoc mesh networking with nearby routers.

A. Personal Container-based Cloudlets

Connecting to the WiFi access point, mobile devices from both rescuers and civilians are able to offload resource-intensive tasks with low latency to the router-based emergency cloudlet. Our system creates, provides and reserves a *personal computing container* A_i (termed *personal cloudlet*) per unique mobile device to ensure secure and privacy-preserving processing of the offloaded (sensor) data. We use *Docker*[1] to handle Linux containers (LXC), which provide lightweight virtualization for personal computing capabilities.

In the following, we describe the offloading process flow (cf. Fig. 1): 1. the mobile device m_i requests the *computing controller* on a specific port for available offloading resources by sending its unique public cryptographic key i and metadata about the offloading task (e.g., type, data size); 2. the

[1]https://www.docker.com (accessed: 2017-04-26)

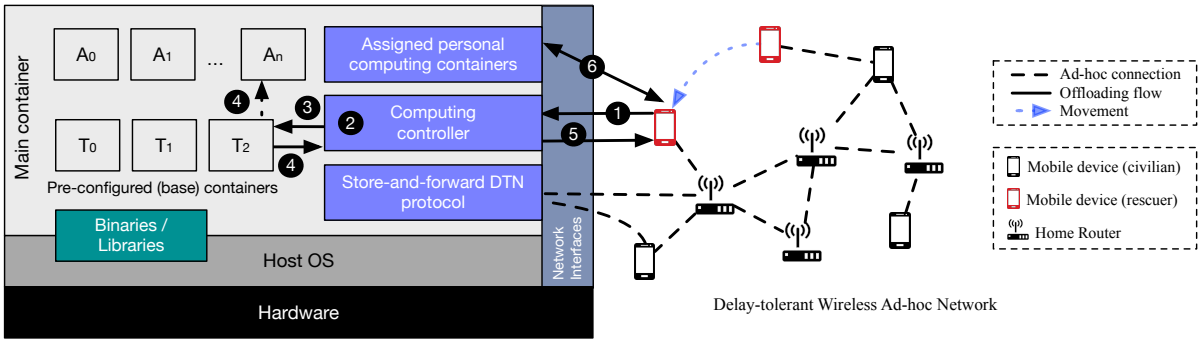

Fig. 1: System design with processing flow and network scenario

computing controller checks the current host's utilization, and - only if free resources are available - lookups in its table whether the mobile client already has an assigned personal computing space A_i or not. 3. if there is no entry yet, the main controller creates a new personal container A_i using a *pre-configured base container template* T_k, which is especially designed for the client's offloading requirements; 4. the created container starts listening on a dynamic port for offloading requests, and sends required data (e.g., container identifier, port, *OAuth 2.0*[2] token for access) to the main controller; 5. the main controller adds a new entry in its table, and sends port info and OAuth token to the mobile device; 6. the device can now directly communicate and offload data to its personal cloudlet container. Idle personal containers are be suspended and reserved for the mobile client until the system runs out of resources or until the configurable timeout period (e.g., 5min) has been reached. In that way, mobile devices can use the assigned personal cloudlet multiple times at short intervals without requiring to create a new container at each time.

By using this router-based offloading opportunity, sensor data can be analyzed directly within the network while mobile devices save valuable energy by conserving own resources [7].

B. Secure DTN Communications

To build a communication bridge between rescuers and civilians, we use a secure *store-and-forward DTN approach* with public cryptographic keys as the primary network identifier as well as the base of a rich security model to ensure confidentiality, integrity and authenticity by design. In [8], the authors already demonstrated the potential of such DTN approach (e.g., with *Serval*) for infrastructure-less communications, and showed its resource efficiency through an extensive experimental evaluation. We chose this approach since IP-based routing is unfeasible in the given network scenario. Moreover, this approach of delay-tolerant communications opens novel ways of distributed in-network processing concepts such as [9]. We plan to research in interconnected cloudlets and integrate the concept of a decentralized computing infrastructure in our system to move the personal computing container along with his assigned mobile user.

[2]OAuth 2.0 is an industry-standard protocol for authorization: https://oauth.net/2/ (accessed: 2017-04-26)

III. Summary and Outlook

In this paper, we developed an upgraded home router as self-sustaining, ad-hoc networking, emergency infrastructure, which provides container-isolated cloudlet functionalities, and acts as secure delay-tolerant communication bridge between mobile devices of involved people (e.g., rescuers, civilians).

In future works, we plan to evaluate different system aspects, and apply our concepts on street lamps for upgrading them as self-sustaining ad-hoc networking device. Utilizing stationary street lamps - one of the densest powered infrastructure in urban environments - we would further extend the proposed complementary emergency infrastructure. Moreover, we will take greater account of the mobility of mobile devices to deliver computational results through the ad-hoc network.

Acknowledgment

This work has been co-funded by the LOEWE initiative (Hessen, Germany) within the NICER project.

References

[1] C. Reuter, A. Marx, and V. Pipek, "Crisis Management 2.0: Towards a Systematization of Social Software Use in Crisis Situations," *IJISCRAM*, vol. 4, no. 1, pp. 1–16, 2012.

[2] Z. Lu, G. Cao, and T. La Porta, "Networking Smartphones for Disaster Recovery," in *PerCom'16*. IEEE, 2016, pp. 1–9.

[3] C. Meurisch, T. A. B. Nguyen, S. Wullkotte, S. Niemczyk, Kohnhäuser, and M. Mühlhäuser, "NICER911: Ad-hoc Communication and Emergency Services Using Networking Smartphones and Wireless Home Routers," in *MobiHoc'17: Poster*. ACM, 2017.

[4] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The Case for VM-based Cloudlets in Mobile Computing," *IEEE Pervasive Computing*, vol. 8, no. 4, 2009.

[5] C. Meurisch, A. Seeliger, B. Schmidt, I. Schweizer, F. Kaup, and M. Mühlhäuser, "Upgrading Wireless Home Routers for Enabling Large-scale Deployment of Cloudlets," in *MobiCASE'15*. Springer, 2015, pp. 12–29.

[6] C. Meurisch, A. Yakkundimath, B. Schmidt, and M. Mühlhäuser, "Upgrading Wireless Home Routers as Emergency Cloudlet: A Runtime Measurement," in *MobiCASE'15: Poster*. Springer, 2015, pp. 338–339.

[7] C. Meurisch, J. Gedeon, T. A. B. Nguyen, F. Kaup, and M. Mühlhäuser, "Decision Support for Computational Offloading by Probing Unknown Services," in *ICCCN'17*. IEEE, 2017.

[8] L. Baumgärtner, P. Gardner-Stephen, P. Graubner, J. Lakeman, J. Höchst, P. Lampe, N. Schmidt, S. Schulz, A. Sterz, and B. Freisleben, "An Experimental Evaluation of Delay-tolerant Networking with Serval," in *GHTC'16*, 2016, pp. 70–79.

[9] T. A. B. Nguyen, C. Meurisch, S. Niemczyk, D. Böhnstedt, K. Geihs, M. Mühlhäuser, and R. Steinmetz, "Adaptive Task-Oriented Message Template for In-Network Processing," in *NetSys'17*. IEEE, 2017.