Sema-IIoVT: Emergent Semantic-Based Trustworthy Information-Centric Fog System and Testbed for Intelligent Internet of Vehicles

Qiaolun Zhang
Shanghai Jiao Tong University

Jun Wu
Shanghai Jiao Tong University

Michele Zanella
Politecnico di Milano

Wu Yang
Harbin Institute of Technology

Ali Kashif Bashir
Manchester Metropolitan University

William Fornaciari
Politecnico di Milano

***Abstract*—In large scale emergency scenarios, massive content for searching, asking for help, and rescue will be generated and transmitted in Intelligent Internet of Vehicular Things (IIoVT). However, IP-networks based emergency systems make rescue decisions on remote emergency centers, leading to inefficient content dissemination and a high-latency response. Moreover, a few previous works address trust issues in the emergency systems, resulting in fake content and malicious emergency services. To address above challenges, we propose an emergent semantic-based information-centric fog system, which realizes trustworthy and intelligent emergency analysis and management. First, we design an efficient emergency content dissemination network for aggregating and analyzing emergency information. Besides, we propose a semantic-based trustworthy routing scheme that filters fake content from malicious entities. Moreover, we implement a real testbed and a simulator to evaluate the benefit and performance of the proposed system. The results show that the proposed system achieves a short average semantic analyzing time and a low failure rate of emergency services.**

I. Introduction

EMERGENCY systems have been deployed around the world to provide emergency services. The early arrival of emergency services is essential to save lives [1]. The current emergency systems are outdated and can not satisfy the time-sensitive need for trustworthy emergency services when natural disasters happen. For example, an earthquake and tsunami in Indonesia in 2018 killed more than 400 and limited road access, leaving the area with no Internet service, which significantly disrupts the delivery of emergency services.

We focus on large emergency scenarios, such as earthquakes, storms, floods, etc., which damage a considerable amount of fibers, data centers, and other communication infrastructures. The emergency system contains emergency communication, information processing, and emergency agent (such as ambulance and fire truck) coordination. With the advent of Intelligent Internet of Vehicular Things (IIoVT) [2]–[4], ubiquitous devices in the edge, such as vehicles, sensors, and road side unit (RSU), bring up new chances to upgrade emergency systems and improve the quality of emergency services. During disasters, a large number of sensors and emergency agents generate a tremendous amount of multi-media content for asking for help, rescue, and emergency resources. These devices, such as RSU and edge servers, provide computing resources for emergency systems to analyze and utilize the rich semantic information for swift rescue.

There are some critical challenges to design new emergency systems. Firstly, it is difficult to disseminate information efficiently and reliably in case that communication equipment (e.g., base station) may be down. Besides, emergency systems suffer from attacks from malicious entities that provide fake content and break the emergency services. For instance, if malicious entities provide fake content about emergency events, emergency agents may go to wrong positions, leaving emergency events unserved. Moreover, most existing emergency systems apply the client-server model, which is not suitable for large scale emergency scenarios. In the client-server model, with most of the rescue agents distributing in the area, asking for help and rescue are on the edge while decisions for emergencies are on the cloud, leading to intolerable rescue delay.

In this sense, we propose the emergent semantic-based trustworthy information-centric fog system, as shown in Fig. 1, which provides emergency services by three components: edge devices, information-centric fog network, and cloud emergency center (CEC). The edge devices collect and pre-process the information on the edge. Besides, the information-centric fog network leverages fog computing [2], [5] to utilize the semantic information for secure emergency analysis and management. With the development of artificial intelligence technology, we can tell a story of emergencies from multi-media content by generating textual summaries [6] in the fog network, which is vital to understand the emergency and disseminate emergency information.

The proposed system communicates using Information-Centric Networking (ICN), which provides resiliency toward infrastructure failure since it does not depend on permanently available or fixed end-to-end paths [7], [8]. Since ICN caches information along the path, information can be retransmitted from one of the replicas. Besides, the rich semantic features can be utilized to increase emergency information dissemination significantly. For instance, the fog network can prioritize traffic based on semantic information and give priority to more urgent information. Also, the cache mechanism of ICN reduces the latency because multiple clients may request the same information. Moreover, we designed semantic-based trustworthy routing mechanisms in fog network to defend against malicious untrusted entities in ICN in the fog networks. The contributions of the proposed system are as follows:

- We proposed a novel emergency communication network, which aggregates and analyzes emergencies with semantic analysis in the network layer.
- We designed a semantic-based trustworthy routing scheme, which filters untrusted content and improves quality of emergency services.
- We proposed a testbed architecture for the proposed system and implemented a sample testbed, which can provide insights to deploy the proposed system on existing IIoVT devices.

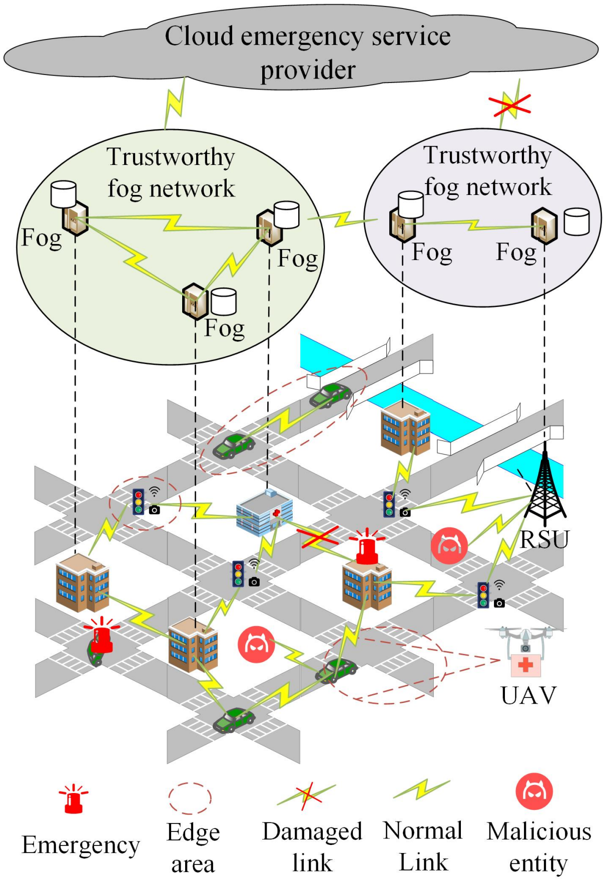


Fig. 1: Our proposed trustworthy information-centric fog system.

The rest of the paper is organized as follows. We first provide an overview of the state of the art. Then we introduce the detailed architecture of the proposed system. Finally, we propose the testbed architecture and evaluation and conclude the paper.

II. Related Works

Many approaches about emergency systems have been studied actively in recent years, which roughly focus on three main branches. (1) *Emergency calls*. This traditional method only provides audio information to the rescuer. (2) *New emergency communications*. Based on edge computing and 5G, these approaches incorporate the capabilities of transmitting multimedia data into the overall management of emergency services. (3) *Reliable Emergency services*. These approaches can provide reliable communications for emergency scenarios [9].

However, there are still critical issues in the existing emergency systems. First, although a device to device system is proposed for safety and emergency services [10], it still relies on fixed access points and lacks an efficient information dissemination scheme. Network infrastructure such as based stations may fail due to natural disasters, leading to disruptions of emergency services in this system. Moreover, only a few works address how to utilize semantic information for emergency services and consider the trustworthiness of the content [11]. Although utilizing fog networks can offer benefits such as low latency, it also brings up security challenges because the fog node can also be exploited by malicious entities. There is no trust management mechanism designed specifically for the emergency system using ICN.

Our proposed system is resilient to the failure of network infrastructure during disasters. Besides, our proposed system analyzes the semantic correlation between massive information and helps to make swift decisions. In addition, the information-centric fog network moves the emergency management intelligence from the cloud to the edge, which reduces the rescue delay. Moreover, the proposed system manages the trustworthiness of content and can resist faked content from malicious entities. The proposed system also utilizes the benefits of 5G. Internet Engineering Task Force (IETF) proposes to enable ICN in 5G core architecture and deploy ICN natively in LTE, 4G mobile networks. ICN can be implemented as a slice of 5G, which supports mass emergency communications using densely deployed base stations.

III. Trustworthy information-centric fog system: Architecture Overview

In this section, we present an architecture overview of the proposed trustworthy information-centric fog system, shown in Fig. 1, organized according to the bi-dimensional resource space presented in [12].

In the proposed architecture, the fog network is connected with the edge devices and the cloud emergency service provider. Different from the client-server model, fog network also coordinates agents for emergencies in the proposed system. During a disaster, enormous emergencies occur around the city. The fog nodes can coordinate agents for emergencies, lessening the burden of CEC. Moreover, the CEC may not know exactly the status of agents and emergencies due to the damage to the telecommunication infrastructure. What's worse is that the CEC may break out during a disaster. The proposed system is resilient to the failure of CEC because the fog network can still aggregate information from edge devices and coordinate agents even if they lost internet connection with the cloud. Besides, fog nodes exchange emergency information with each other to improve coordination performance. Derived from the ICN publish-subscribe paradigm, the information dissemination mechanism in the proposed system employs two types of packets: (a) the interest (or request) packet to retrieve a specific category of content and (b) the data packet to provide content to the requester. The information-centric fog network utilizes ICN to provide the following advantages. First, it provides resiliency because it does not require a centralized server. In addition, thanks to the cache scheme of the information-centric fog network, information can be transmitted from one of the replicas if the publisher is down. Besides, it also contains rich semantic information, which can be utilized to improve emergency information dissemination efficiency significantly. Moreover, the information-centric fog network offers low latency due to its cache mechanism.

As shown in Fig. 1, at the lowest level, edge devices can provide storage and computing capabilities, which can be utilized to pre-process the information received across the area. These devices generate content about the emergency and act as a data publisher. Conversely, the emergency agents can subscribe as a consumer for particular emergency categories, basing on their reaction capability. This second layer has three main functions: (1) interacting with edge devices, (2) communicating with other fog nodes, and (3) interacting with the CEC. When information about emergencies arrives, fog nodes exploit the semantic feature of ICN to extract the types, required agents, and time constraints of emergencies. Then, fog nodes publish emergency information as content and distribute them among fog nodes according to the corresponding subscription they made. After analyzing the information, the fog network coordinates agents to handle the emergencies and sends the information of unsolved emergencies to the CEC.

Since all the devices in the IIoVT and the surroundings can publish and request content, the system may suffer from faked content from malicious entities. Faked content can destroy emergency services. For instance, the faked position of emergency events can mislead the ambulance to the wrong place. To detect the faked content, we design mechanisms for fog networks to determine the trustworthiness of the content. The fog nodes determine the direct trustworthiness of devices based on their interactions with the devices and the information from other fog nodes. Then the fog nodes evaluate the trustworthiness of the received content and filter malicious content from untrustworthy entities.

IV. Semantic-based Efficient Trustworthy Content Dissemination Scheme

In this section, we propose a novel efficient trustworthy content dissemination scheme based on semantic analysis for the proposed emergency system.

A. Overview of Trustworthy Emergency Content Delivery

Nowadays, with the increasing number of IIoVT devices around the city, research and enterprise communities are taking into account the usage of the computing and communication resources at the edge of the network [5]. These devices provide computation and communication resources for the emergency system.

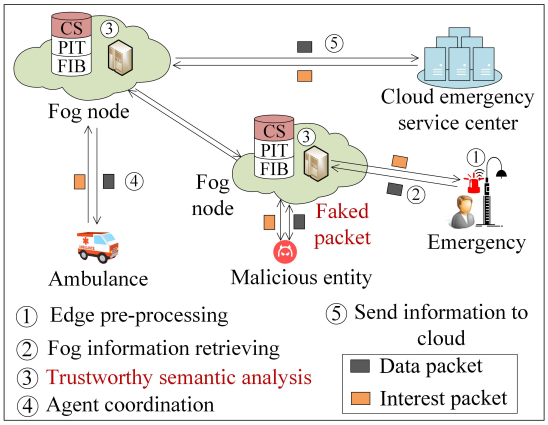


Fig. 2: Trustworthy emergency content delivery.

Fig. 2 illustrates the emergency content delivery in the proposed system. First, the ambulance sends an interest packet to the fog node nearby for information of patients in danger. After that, a smart lamp discovers a person in danger. It videotapes the person and broadcasts the information to the fog nodes in the vicinity. Then the node sends an interest packet to the smart lamp and requests for emergency information(e.g., locations, audios, videos). After receiving the data packet, the fog node extracts text from multi-media data by image captioning and video captioning. In the meantime, there is a malicious entity sending faked packets to the fog node. The malicious entity can send faked interest packets or publish forged data packets. On the one hand, the malicious entity can send faked interest packets for information of patients in danger, which fools the fog node to dispatch the emergency event to itself. On the other hand, the malicious entity can publish data packets containing forged emergency events, misleading it to dispatch the emergency event to itself. To defense against these attacks, the fog node analyzes the semantic information and judges the trustworthiness of the entity. If the entity is not trustworthy, the fog node discards the packet directly. Otherwise, it adds the analyzing result to the content name. After extracting the information, the fog nodes check if there are agents that can arrive before the deadline. If there are agents found for the emergency, the fog network sends the information to the agents. Otherwise, the

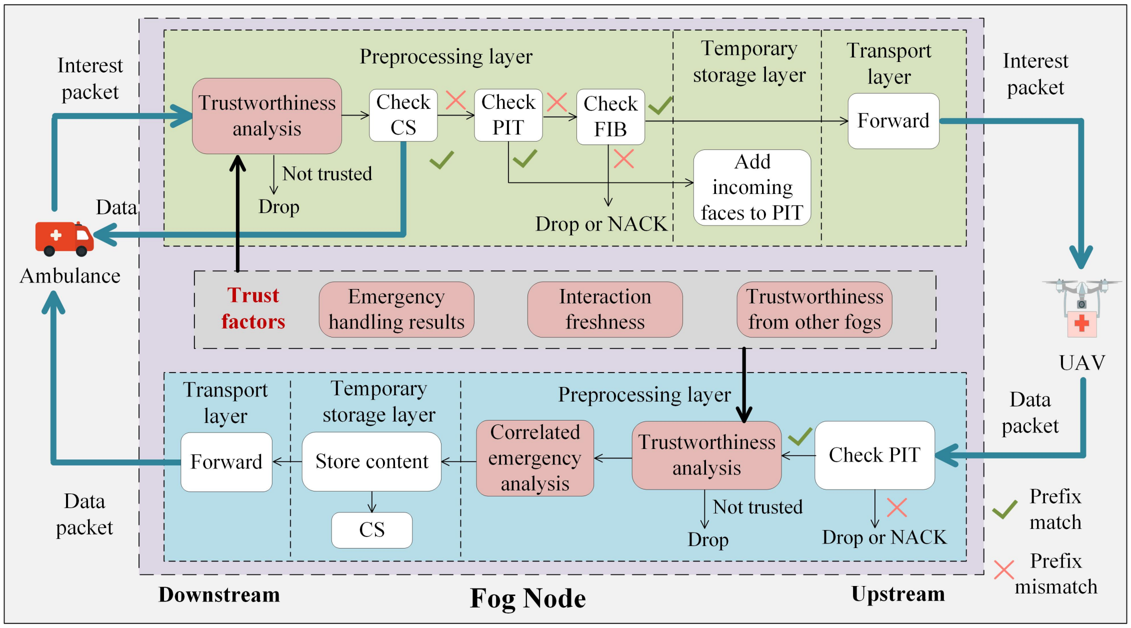


Fig. 3: Semantic-based trustworthy routing of fog nodes.

information is sent to the CEC. At last, the agents handle the corresponding emergencies.

B. Semantic-based Trustworthy Routing Scheme

According to the existing fog computing paradigm [5], we propose the structure of fog node, which applies ICN in emergency scenarios. Routing in the fog node is shown in Fig. 3. Each fog node maintains three data structures to transmit the packets. A *Forwarding Information Base* (FIB) keeps track of the routing information of the various interest packets. A *Pending Interest Table* (PIT) keeps states of the forwarded interest packets. The fog node analyzes the semantic information of incoming data packets and caches the analyzed information in a *Content Store* (CS). When receiving multi-media data, the fog node generates textual summaries [6], which significantly reduces the amount of traffic in the system. The fog node decides whether to transmit multi-media data according to the trustworthiness of the sender, the request of the client, and the emergency type. During transmission, the fog node adopts a dynamic naming approach and adds new fields to the content name after analyzing the content.

The fog node consists of six layers. In the *physical and virtualization layer*, the node uses the IP network to build an overlay network or directly uses hardware to implement ICN. The *monitoring layer* watches hardware status. The *pre-processing layer* analyses the emergencies and schedules agents for emergency rescue. Moreover, the *pre-processing layer* performs trustworthiness analysis on the entity that sends the packet. The fog node measures the trustworthiness of an entity by emergency handling results, interaction freshness, and trustworthiness from other nodes. If the fog node successfully handles one emergency using the information published by one entity, the corresponding entity is more trustworthy. Since the trustworthiness of one entity may change over time, the more recent interactions contribute more to the trustworthiness of an entity. The fog node also combines the trustworthiness from other nodes because it may not have full knowledge about the entity. After performing the trustworthiness analysis, the fog node figures out correlated emergencies using semantic information, which is vital for determining the types and quantity of emergency agents. In addition, when the fog node can not deal with all emergency traffic, it utilizes semantic information to determine the importance of emergencies and delays forwarding the interest packets for the unimportant emergencies, reducing the corresponding data packet and improving the quality of service (QoS) of more urgent information. The *temporary storage layer* caches the analyzed information about agents and emergencies. The *security layer*, instead, comes into play for sensitive information. Finally, the *transport layer* forwards the packets to the corresponding receiver.

C. Fog-enabled Emergency Information Extraction and Agent Coordination

In this section, we first discuss the emergency information extraction based on the semantic features of ICN. Then we propose the agent coordination using the information obtained in the fog node.

The emergency information includes semantic information about the agents, emergency events, and constraints for coordination, such as traffic conditions. The fog node can utilize image captioning and video storytelling to generate textual summaries for emergency events [6], which is further analyzed to figure out the type and urgency of emergencies. Then the fog node gets the types of required agents and estimates the time limit to handle the emergency. Similarly, the fog node gets the types and positions of emergency agents. These analyzed results will be added to the content name. The fog node classifies the information according to the content name of the packet, which is named according to the hierarchical naming structure of ICN [7] and contains rich semantic information. For instance, a sample content name is defined as /shanghai/patient/injured/minhang/severe/video/demo.mpg, which means that there is a seriously injured person in Minhang. Then, the fog node extracts the sensor data from edge devices to analyze the traffic condition using methods proposed in [13]. For example, based on the GPS data, the fog node estimates the speed of the agent between two positions.

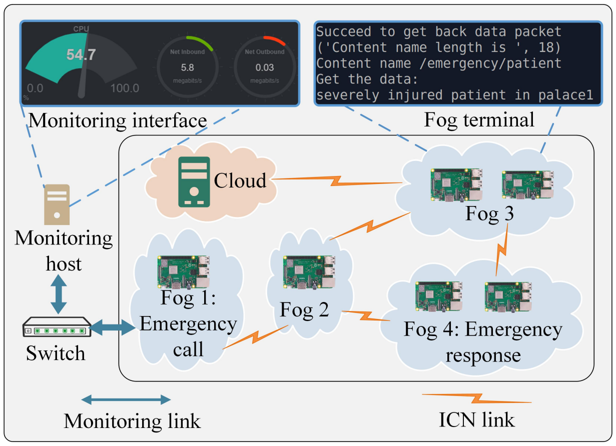
After gathering all the information, the fog nodes coordinate the available agents to deal with the emergency. We formalize the agent coordination problem as an assignment problem. The fog node assigns the agents available to emergency events to minimize the damage caused by all emergency events. The traffic condition, road condition, time limit, and available agents are the constraints for the problem. First, according to the emergency type, the fog node figures out the agents that are capable of handling the corresponding emergency. Second, the fog node utilizes the road condition, distance, and speed between the position of the emergency event and the agent to estimate the time for the agent to arrive. Finally, the fog node selects agents according to the constraints mentioned above.

V. Testbed Architecture

In this section, we propose a testbed for the proposed system, which provides some insights to deploy the proposed system using existing IIoVT devices.

A. Overview and Architecture of the Testbed

The testbed has two separate networks: emulation network and monitoring network. The emulation network simulates the connection between the fog nodes using ICN. We implemented an overlay network using Python according to Named Data Networking (NDN) [7], and the analytic model of ICN [3]. NDN is an instantiation of ICN, and the analytic model of ICN exploits more mechanisms for emergency scenarios. This implementation consists of three parts: overlay ICN network, hardware status monitoring, and virtual fog node. The overlay ICN network is on top of the TCP/IP network. We implemented PIT, CS, and FIB for the forwarding process. We define pre-defined FIB tables for each device to provide initial virtual connections among devices in the system. The FIB table is updated after receiving new interest packets. Moreover, the fog node applies a modified method to forward the packet. Specifically, it only forwards the data packet to the selected agent rather than all the agents matching the PIT. Besides, the fog node adds more fields to the content name after analyzing it, which makes the content name contain more information. Multiple devices provide resources for a virtual fog node. One device acts as a controller to coordinate the other devices that make up this fog node. One control device in the fog node coordinates all the other nodes in the system. The monitoring network manages and monitors the performance of the testbed including the CPU utilization, bandwidth, memory usage, etc. The testbed can use any device with two network cards. We choose the Raspberry



```
Succeed to get back data packet
('Content name length is ', 18)
Content name /emergency/patient
Get the data:
severely injured patient in palace1
```

Fig. 4: An overview of testbed architecture.

Pi for our testbed due to its reduced cost. Fig. 4 depicts an overview of the testbed architecture for the proposed system. The emulation network and monitoring network use the wireless network card and the wired network card, respectively. All Raspberry Pi devices and a monitoring host computer are fully interconnected. In this way, the researcher can send commands to the monitoring host, which makes configurations of the Raspberry Pi devices. After initial configuration, Raspberry Pi devices form a fog network and communicate through wireless network communication. Fog nodes can also send their current status information to the monitoring host computer, which instantiates a virtual network topology and provides information to the researcher.

B. Testbed Configuration and Status Monitoring

To effectively configure the testbed, we utilize the monitoring network, which is connected using a switch. Since this network and the emulation network are separate, they don't interfere with each other. All the Raspberry Pi devices and the monitoring host can connect with each other using the IP address. The monitoring host is used to deploy arbitrary network topology to the testbed. In the implemented overlay network demo, the fog nodes load FIB from the configuration file, which sets up the emulation network topology. To adapt the demo code to specific scenarios, we need to modify the configuration file and add the interactions among the hosts and the fog node. Besides, after enabling status monitoring in the configuration file, fog nodes will send two types of information to the monitoring host: the hardware status and the packet status. In specific, the fog node sends the hardware status (e.g., CPU utilization rate, CPU temperature) periodically. While, once the fog node receives or sends a packet, it sends the packet status to the monitoring host.

VI. Experimental Evaluation

This section aims to discuss the performance of the proposed system using the proposed testbed and a customed simulator based on EdgeCloudSim [14]. The evaluation results of the testbed are used in the simulation tool to get results for a large topology. The simulation part is performed using a custom extended version of the simulation tool EdgeCloudSim [14]. Specifically, we added a module that simulates emergency agents to handle emergencies.

We consider a 3 hours emergency rescue scenario under an earthquake and assume that all the emergencies are time-sensitive. The simulated area is $10,000$ square kilometers with 200 rescue teams at the beginning. The simulation uses a discrete event management framework and models the emergency and rescue during simulation time in every second. We assign different speed of occurrence of emergency events to different areas. During the rescue, we can send rescue teams from the emergency center or the area of the earthquake to newly occurred emergencies. We evaluate the performance of the system by increasing the number of emergencies from $20,000$ to $120,000$ in the simulation time. The data size in simulation ranges from 250 KB to 2500 KB, which is enough to transmit a small compressed video. The average data size is 1800KB, which results in traffic rate in an edge device from 120 MB/h to 2200 MB/h.

We compared the semantic analyzing time of three different cache strategies, namely, first in first out (FIFO), least-frequently used (LFU), and least recently used (LRU). As stated in [15], the popular content in ICN follows the Zipf's law, in which alpha indicates the intensity of the popularity distribution. Fig. 6 shows the average semantic analyzing time under different cache mechanisms when we increase alpha. The analyzing results can

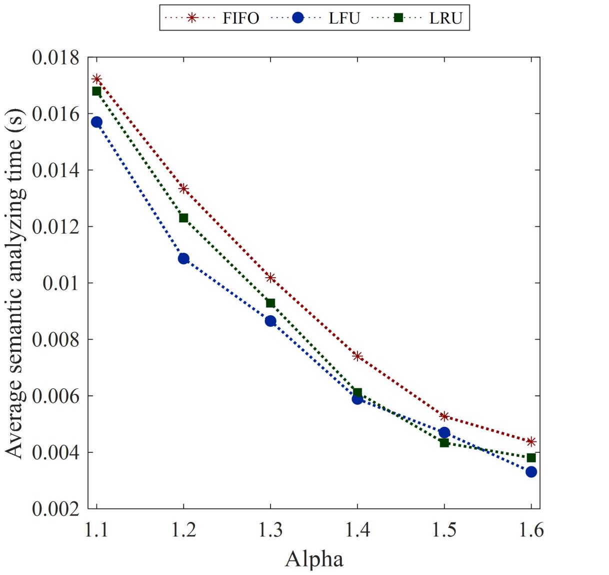


Fig. 5: Average semantic analyzing time versus Zipf exponent.

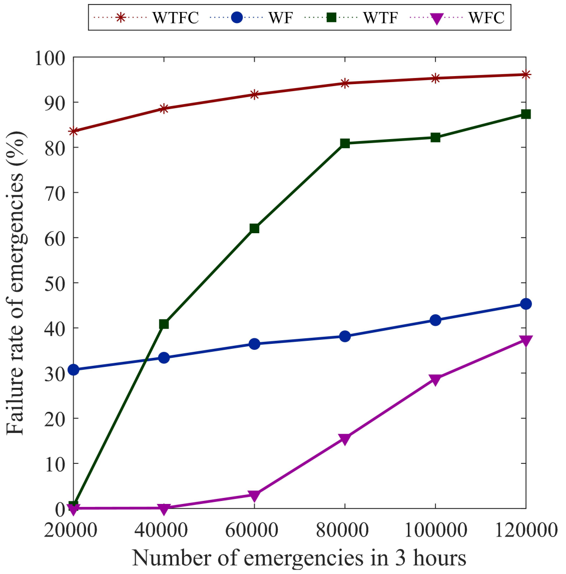


Fig. 6: Failure rate versus emergency number.

be cached to reduce the analyzing time of the packet. For each cache strategy, the number of processed data packets is 3000. Results show that the average semantic analyzing time decreases as alpha increases because the previous cached results are more likely to be reused. Besides, FIFO has the longest analyzing time. LRU is better than LRU when alpha is less than or equal to 1.4. When alpha is greater than 1.4, there is no big difference between LFU and LRU.

We simulated four scenarios to show the performance of the proposed system. The first three scenarios all utilize the proposed system and differ in what is down during the earthquake. The first scenario is the proposed system without fog networks and cloud (WTFC). In WTFC, the base stations lost connection with each other, and the backhaul links are down. The second scenario is the proposed system with working fog networks (WF), in which all the backhaul links are down, and the fog can not access CEC. However, the fog nodes can connect with each other. The third scenario is the proposed system with working fog networks and cloud (WFC), which is an ideal case that the network is not damaged. The last scenario is the traditional system without fog networks (WTF), in which clients directly connect with CEC. Fig. 6 shows the simulation results. The failure rate of WTFC is highest while the one of WFC is lowest. The failure rate of the WF scenario is higher at the beginning because the emergency agents (e.g., rescue teams) cannot connect with CEC, and they only rely on the fog node to coordinate them. However, since the fog network can fully utilize the emergency teams in the system, WF performs better than WTF as the number of emergencies increases. Using both fog and CEC, the failure rate of the traditional client-server system decreases from 87% to 37%. The failure rate of the WF scenario is higher at the beginning because there is no cloud available to fully utilize the rescue teams from the emergency center.

VII. Conclusions and Future Works

In this paper, we propose a rapidly deployable trustworthy emergency service system for IIoVT. Firstly, we present an intelligent emergency content dissemination network to efficiently transmit and analyze emergency information in IIoVT. Secondly, we present a semantic-based trustworthy routing scheme to filter malicious content from untrustworthy entities. Finally, we propose a testbed architecture to evaluate some scenarios to show that the proposed system achieves promising performance for handling emergency events.

Starting from this work, there are some future research issues. We are investigating how to fully utilize the semantic features of ICN. Besides, it is worthwhile to deploy the system and conduct large-scale experiments in a real-life emergency scenario.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 61831007, 61972255. This work is supported by Shanghai Key Laboratory of Integrated Administration Technologies for Information Security. The corresponding authors of this paper are Jun Wu (junwuhn@sjtu.edu.cn) and Wu Yang (yangwu@hrbeu.edu.cn).

References

[1] I. Hasselqvist-Ax, G. Riva, J. Herlitz, M. a. Rosenqvist, J. Hollenberg, P. Nordberg, M. Ringh, M. Jonsson, C. Axelsson, and J. Lindqvist, "Early cardiopulmonary resuscitation in out-of-hospital cardiac arrest," *New England Journal of Medicine*, vol. 372, no. 24, p. 2307–2315, 2015.

[2] P. Corcoran and S. K. Datta, "Mobile-Edge Computing and the Internet of Things for Consumers: Extending cloud computing and services to the edge of the network," *IEEE Consumer Electronics Magazine*, vol. 5, no. 4, pp. 73–74, Oct. 2016.

[3] J. Yang, Y. Sun, and Y. Cao, "An Analytical Model for Information Centric Internet of Things Networks in Opportunistic Scenarios," *IEEE Systems Journal*, 2019.

[4] M. U. Ghazi, M. A. Khan Khattak, B. Shabir, A. W. Malik, and M. Sher Ramzan, "Emergency Message Dissemination in Vehicular Networks: A Review," *IEEE Access*, vol. 8, pp. 38 606–38 621, 2020.

[5] M. Aazam and E. Huh, "Fog Computing: The Cloud-IoT\/IoE Middleware Paradigm," *IEEE Potentials*, vol. 35, no. 3, pp. 40–44, May 2016.

[6] J. Li, Y. Wong, Q. Zhao, and M. S. Kankanhalli, "Video storytelling: Textual summaries for events," *IEEE Transactions on Multimedia*, vol. 22, no. 2, pp. 554–565, Feb 2020.

[7] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, p. 66–73, 2014.

[8] M. Aibin, M. Kantor, P. Boryło, H. Niedermayer, P. Chołda, and T. Braun, "Resilient SDN, CDN and ICN Technology and Solutions," in *Guide to Disaster-Resilient Communication Networks*, ser. Computer Communications and Networks, J. Rak and D. Hutchison, Eds. Cham: Springer International Publishing, 2020, pp. 631–652.

[9] N. Zhao, W. Lu, M. Sheng, Y. Chen, J. Tang, F. R. Yu, and K.-K. Wong, "UAV-Assisted Emergency Networks in Disasters," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 45–51, Feb. 2019.

[10] U. Albalawi, "A Device-to-Device System for Safety and Emergency Services of Mobile Users," *IEEE Consumer Electronics Magazine*, vol. 8, no. 5, pp. 42–45, Sep. 2019.

[11] V. Tundjungsari and H. Yugaswara, "Supporting collaborative emergency response system with reputation-based trust peer-to-peer file sharing," in *2015 International Conference on Technology, Informatics, Management, Engineering Environment*, Sep. 2015, pp. 6–11.

[12] M. Zanella, G. Massari, A. Galimberti, and W. Fornaciari, "Back to the future: resource management in post-cloud solutions," in *Proceedings of the Workshop on INTelligent Embedded Systems Architectures and Applications*. ACM, 2018, p. 33–38.

[13] A. Thakur and R. Malekian, "Fog Computing for Detecting Vehicular Congestion, an Internet of Vehicles Based Approach: A Review," *IEEE Intelligent Transportation Systems Magazine*, vol. 11, no. 2, pp. 8–16, 2019.

[14] C. Sonmez, A. Ozgovde, and C. Ersoy, "Edgecloudsim: An environment for performance evaluation of edge computing systems," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 11, p. e3493, 2018.

[15] M. Hajimirsadeghi, N. B. Mandayam, and A. Reznik, "Joint Caching and Pricing Strategies for Popular Content in Information Centric Networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 654–667, Mar. 2017.

Qiaolun Zhang is a master student in School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. Contact him at zhql0907@sjtu.edu.cn.

Jun Wu is currently a professor of and the vice dean of Institute of Cyber Science and Technology, Shanghai Jiao Tong University, China. Contact him at junwuhn@sjtu.edu.cn.

Michele Zanella is currently a PhD student at the Department of Electronics, Information and Bioengineering, Politecnico di Milano, Italy. Contact him at michele.zanella@polimi.it.

Wu Yang is currently a professor with Harbin Engineering University. His research interests include cyber security, P2P network, and Internet of Things. Contact him at yangwu@hrbeu.edu.cn.

Ali Kashif Bashir is a Senior Lecturer at the Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom. He is also with National University of Science and Technology, Islamabad (NUST), Islamabad, Pakistan. Contact him at dr.alikashif.b@ieee.org.

William Fornaciari is a professor at the Department of Electronics, Information and Bioengineering, Politecnico di Milano, Italy. Contact him at william.fornaciari@polimi.it.