EAI Endorsed Transactions
on Context-aware Systems and Applications

Research Article **EAI.EU**

Context-Aware Mobility in Internet of Thing: A Survey

Vu Tuan Anh[1,*], Pham Quoc Cuong[2], Phan Cong Vinh[3]

[1]Faculty of Electronics Technology, Industrial University of Ho Chi Minh City, Ho Chi Minh City, Vietnam. Email: vutuananh@iuh.edu.vn
[2]Faculty of Computer Science and Engineering, Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam. Email: cuongpham@hcmut.edu.vn
[3]Faculty of Information Technology, Nguyen Tat Thanh University, Ho Chi Minh City, Vietnam. Email: pcvinh@ntt.edu.vn

Abstract

The rapid growth in Internet of Thing (IoT) yields big data that require management, computing, authentication, and analysis. In the first step of IoT, the static things are connected together such as: sensors, cameras, vending machine and so on. The things just need static IP address to manage and collect data easily. The next step of IoT, the mobile things such as: cellphones, patients, vehicles and so on are more difficult. Besides the dynamic IP, the mobility things yield challenges to mobile data collection, mobile data analysis, energy management, and security and privacy. In this paper, we make a survey of context-aware mobility in IoT. First, The mobile data collection means the contexts of users that are collected due to cellphone, or google android devices, have ability to send a signal over mobile network. Next, The mobile data analysis helps to classify the context for authenticating and analyzing. The energy management helps battery of devices to work in the long time and improve effect of the communication in IoT. All processes need a framework as MobilityFirst Future Internet Architecture. The final challenge in IoT is security and privacy infrastructure when the mobile things move from one area to another.

Received on 20 February 2019; accepted on 23 February 2019; published on 18 March 2019

Keywords: IoT, Context-Aware in IoT, Mobility in IoT, MobilityFirst

doi:10.4108/eai.13-7-2018.158875

1. Introduction

The internet is made to transfer data in global network. The data can be picture, document file, and information. Due to development of computing and sensors, The things, such as vehicle, cellphone, cameras and so on, are connected to internet to get information for special purposes as controlling traffic, healthcare, agriculture, vending machine and so on. Internet of Thing (IoT) make a thing having ability to connect to internet via wire or wireless network. Beside the authentication and security, the context aware is researched and developed widely. The next step of this scenario is Internet of Mobile Things (IoMT) [7]. Some challenges when deploy IoMT are mobile data collection, mobile data analysis, energy management, security and privacy, and delivery IoT services. For collecting mobile data, we need a future Internet architecture as MobilityFirst [10]. Mobility are thing that can change IP address over network areas. After moving of users, the system need to clean IP address for next using. MobilityFirst is framework with protocols to support the communication between devices in IoMT. Next step is context aware authentication for managing and analyzing [3]. In the end, mobile data is forwarded and delivered. All processes of IoMT will be demonstrate in the figure 1.

*Corresponding author. Email: vutuananh@iuh.edu.vn

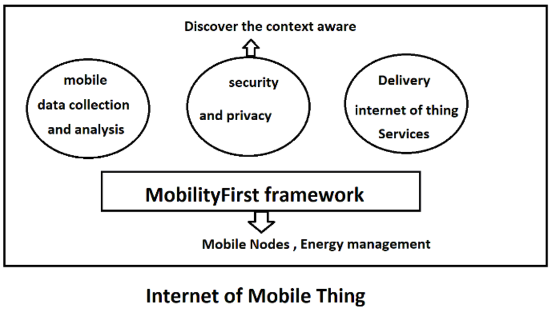

Figure 1. All processes of IoMT

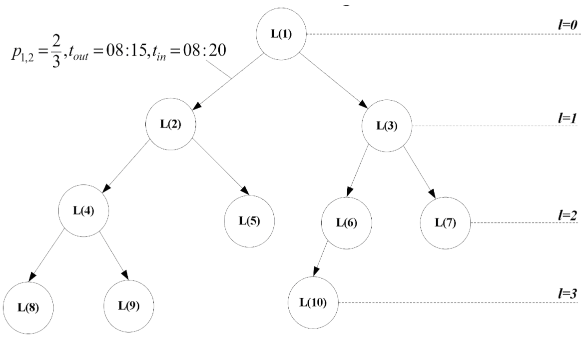

Figure 2. Mobile probability tree [1]

2. Mobile Data Collection

To collect data in mobile network, the nodes network need some algorithm to optimize the communication. Mobility-aware nodes are needed.

2.1. Mobile nodes

Every things in IoT have sensors that have ability to send wireless signal, or bluetooth signal to the center. Wireless sensor network (WSNs) are devices to collect data in IoT [2]. The mobile nodes is protocol solution for WSNs with the mobility-related signaling. First step, we need to manage mobility IP on Ipv4 protocol that is updated on Ipv6 version. In the packet, it includes Ipv6 header, Ipv6 address with 128 bits or 16 bytes length size of address.

The next step is routing over WSNs when we need to discover neighbor nodes. Ipv6 address must have ability to reconfigure IP automatically to meet mobility characteristic in Ipv6. Some challenges in Ipv6 are larger size of header, dedicated bandwidth, global addressing scheme, implementation issues, and transport protocol. After receiving the packet, the nodes social relations cognition need to be solved for classifying and authenticating.

2.2. Nodes social relations cognition

The basic of communication in mobility-aware is nodes mobility and random. Following the work in [1], the difficulty of data-awareness and data-transmission is the mobility of the nodes in the network. The work yields out algorithm which bases on the mobile node by calculating the quantization social relation of mobile nodes. The results of this process is mobile probability tree as in figure 2:

Then, mobile nodes are classified in subgroups and probability tree to predict the way of mobile node. That means the nodes must be met strong social relationship, high density of interconnection.

Finally, awareness service nodes are determined in the objective regions, through trust-transference and probability calculation.

However, this work still lack of global awareness service center to get real-time access and automated analysis. All results in this work have just done in simulation (by Matlab software) and lack of evaluation in the real life.

3. Mobile Data Analysis

In [7], to characterize mobile thing such as where, what and which devices, we need GPS sensors. Next, the mobility characterization is implemented on UIM Traces. Besides, authors also model mobility due to mobility characterization to create Support Vector Machine (SVM). SVM helps to build binary classifiers to classify the communication between two devices. SVM helps to predict the missing contact and future movement due to regular patterns of users. The prediction includes location predictor, stay duration predictor, and contact predictor. After that, the sensing devices selection and content distribution happen. The results in this work are good in location prediction and contact prediction. However, the duration prediction accuracy is not a good result. The more researching on this area needs to be done to give out more exactly evaluation.

4. Energy Management

In IoMT, the energy management is an important thing to be improved to extend the battery time. The different in types of mobile thing yields out some difficult. There are three features we need to solve: energy source placement, energy exchange, and cross-device energy management and monitoring [7]. In [7], authors just focus on the first feature. The solution is electric of the vehicles. The authors also give out wireless charging solution for mobile thing. The charging pads are installed under the road when the cars move over them and get good results in maximum flow charged under various situations. The remaining features including: energy exchange and cross-Device energy management need more research in the futures. Also, we need an algorithm to turn on or turn off the charging pads to save energy. Hope there will be some research on it in the future.

5. Security and Privacy

In [1], the devices have a changing in security and privacy when they move over the mobile nodes. The devices need to be recognize and authenticate as new devices. That means they need a new IP for next action. In the new environment, the data packet must be met the new standard in context (in different type or in different size of data). The last, there is maybe new preserving location privacy. All processes need a framework for authenticating.

MobilityFirst Architecture is a such framework to be used to emerging mobile Internet applications with some attributes, such as name, address, public-key for authentication [9]. Design goals of this work are:

- Seamless host and network mobility (smoothly continuous or uniform in quality). The host is identified by an IP address
- No single root of trust (single authority)
- Intentional data receipt (the receiver has ability to reject or accept incoming traffic)
- Proportional robustness
- Content addressability
- Evolvability (deploy rapidly on new services)

Another field in researching MobilityFirst is trustworthiness that means the network has ability to resilience to reduce the malicious endpoint or network router [10]. MobilityFirst needs to clean separating name or identifier and enhance security.

This is self-certifying without third-party certification. Simply, the key is just a public key that encrypted using private key. All protocols of the authentication process are yielded in this work. Beside, the work also gives out a solution to enhance network functions with handling endpoint mobility.

The handshake is established via 4 steps: pre-lookup, connect-time, individual, and simultaneous that are demonstrated in figure 3. To handle mobility, we need to classify things in three categories:

- In direction
- Global name resolution
- Name-based routing

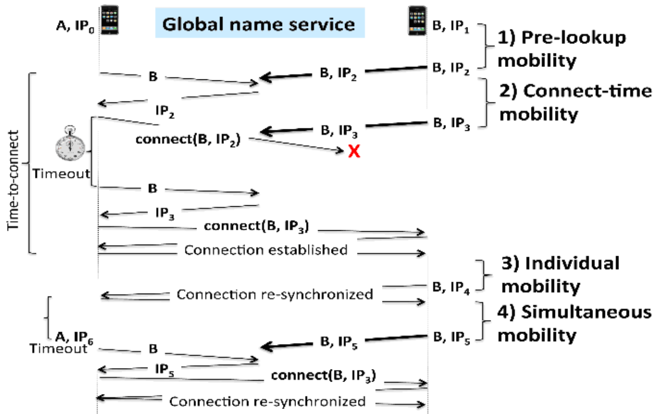

Figure 3. Four kinds of mobility [10]

In the next step, MobilityFirst needs a cloud-inspired service for sensors [4]. The name is Sensing-as-a-Service (S^2aaS) that can supply a crowdsourced data to run application on a cloud platform. In this work, the authors propose mobility-aware crowdsourcing (MACS) framework providing S^2aaS to smart city management platform. The solution helps us to deploy more applications in the smart city. However, the work just uses the simulation for the algorithm and is needed more applications in the real city. The evaluation is more exactly in practical city. The final step, MobilityFist needs an algorithm to discover the context-aware resource, and then deliver IoT services. The more details of them are yielded in [6, 8].

6. Discovering Context-Aware

Discovering the context helps to resilience of contact that maybe not present at that time to save the energy. The authors in [8] introduce a context-aware resource discovery (CARD) framework to extend the functionalities of asynchronous neighbor discovery protocols. The neighbors need to be guaranteed to present to communicate. The protocol allows two devices to discover each other in the same instant of time. Due to this CARD, the system can determine mobility pattern, calculating total cumulative residual contact time, total energy consumed for the discovery process, and average latency for the discovery process. The CARD uses machine learning technique (so called, Q-learning) to help reducing energy consumption. The CARD can be applied in the smart building and smart cities deployment. However, the authors also give out the future work as improving the realistic mobility pattern, and deploying on large system with the numerous devices.

7. Delivering IoT Services

In [5], the authors introduce mobiiscape software to support scalable mobility pattern monitoring of moving objects in large-scale city. This software demonstrates how to distribute IoT services. Said in [6], MobilityFirst's identity based routing, overloaded identity resolution, content caching and in-network compute plane are excellent to build blocks for IoT service distribution. The authors in [5] explain that each service needs a GUIs, stored RDF graph of C1 to network address mapping. For more imaging in the mind, the figure 4 of this work will show this

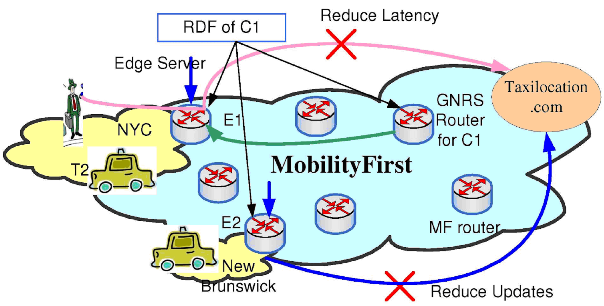

Figure 4. IoT service as the in-network service of Mobility-First [6]

For example, taxi service has own GUIs (C1) to communicate with the customers and the drivers and be set at the edge server (website: taxilocation.com). It also has RDF C2 (relative website: mobile.verizon.com). While C1 relates to public key for authentication, C2 is known as reference for C1 with a location due to GPS value. This is also a scenario of a location context-aware IoT service in RDF graph (Standard Middleware API). This work also yields out an algorithm to optimize the storage and compute planes for MF router, related to Web, sensors, and apps. MF router architecture has a service caching that includes data block for GUIs. However, this work has no deployment in the real life. The authors just have a future work demonstrating WSNs to determine the location of nearby cab by RFID tag inside each phone. RFID tabs constant GPS and sends the location to the center system. The nearby metric is calculated from this signal. With the algorithm, we can apply on the other services in the real life as traffic, location of patient in an emergency situation and so on.

8. Future Work and Conclusions

The internet is made to transfer data in global network. The data can be picture, document file, and information. After that, when we need more information of things as vehicle, vending machine, patient for analyzing, calculating, or just storing, the sensors with android system are tag inside the things to collect information of mobile things and send them to the data center later for analyzing. The IoMT also yields out some challenges in mobile data collection, mobile data analysis, energy management, security and privacy, and delivering IoT service. The first, mobile data collection needs mobile nodes architecture to collect data. The reference of it is in [1, 2]. This research in mobile data collection needs more practicing in the real life to get more exact evaluation. Next, the data are analyzed as in [7], and still need to improve duration prediction accuracy results. The other challenge of IoMT is energy management to maintain the long life of batteries. The work in [7] gives out the solution for charging the battery including wire and wireless. However, an algorithm needs to be researched for turn on and off the charging pad to save more energy. With the security and privacy, we can refer in [1, 4, 9, 10] that give out the solution and algorithm but they lack of deploying in the real life. The final step, MobilityFist needs an algorithm to discover the context-aware resource, and then deliver IoT services. The more details of them are referred in [6, 8]. In the future research, IoT needs to deploy with numerous devices and other services.

References

[1] Jian An, Xiaolin Gui, Wendong Zhang, and JinHua Jiang. Nodes social relations cognition for mobility-aware in the internet of things. In *Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, ITHINGSCPSCOM '11, pages 687–691, Washington, DC, USA, 2011. IEEE Computer Society.

[2] Safwan M. Ghaleb, Shamala Subramaniam, Zuriati Ahmad Zukarnain, and Abdullah Muhammed. Mobility management for iot: a survey. *EURASIP J. Wireless Comm. and Networking*, 2016:165, 2016.

[3] Kashif Habib and Wolfgang Leister. Context-aware authentication for the internet of things. In *Proceedings of The Eleventh International Conference on Autonomic and Autonomous Systems (ICAS)*, pages 134–139. IARIA, 2015.

[4] Burak Kantarci and Hussein T. Mouftah. Mobility-aware trustworthy crowdsourcing in cloud-centric internet of things. In *IEEE Symposium on Computers and Communications, ISCC 2014, Funchal, Madeira, Portugal, June 23-26, 2014*, pages 1–6, 2014.

[5] Byoungjip Kim, Sang Jeong Lee, Youngki Lee, Inseok Hwang, Yunseok Rhee, and Junehwa Song. Mobiiscape: Middleware support for scalable mobility pattern monitoring of moving objects in a large-scale city. *Journal of Systems and Software*, 84(11):1852–1870, 2011.

[6] Jun Li, Yan Shvartzshnaider, John-Austen Francisco, Richard P. Martin, Kiran Nagaraja, and Dipankar Raychaudhuri. Delivering internet-of-things services in mobilityfirst future internet architecture. In *3rd IEEE*

International Conference on the Internet of Things, IOT 2012, Wuxi, Jiangsu Province, China, October 24-26, 2012, pages 31–38, 2012.

[7] Klara Nahrstedt, Hongyang Li, Phuong Nguyen, Siting Chang, and Long Vu. Internet of mobile things: Mobility-driven challenges, designs and implementations. In *Proceedings of The First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pages 25–36. IEEE, 2016.

[8] Riccardo Pozza, Michele Nati, Stylianos Georgoulas, Alexander Gluhak, Klaus Moessner, and Srdjan Krco. CARD: context-aware resource discovery for mobile internet of things scenarios. In *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2014, Sydney, Australia, June 19, 2014*, pages 1–10, 2014.

[9] Dipankar Raychaudhuri, Kiran Nagaraja, and Arun Venkataramani. Mobilityfirst: A robust and trustworthy mobility-centric architecture for the future internet. *SIGMOBILE Mob. Comput. Commun. Rev.*, 16(3):2–13, December 2012.

[10] Arun Venkataramani, James F. Kurose, Dipankar Raychaudhuri, Kiran Nagaraja, Morley Mao, and Suman Banerjee. Mobilityfirst: A mobility-centric and trustworthy internet architecture. *SIGCOMM Comput. Commun. Rev.*, 44(3):74–80, July 2014.