

EDITORIAL

Open Access



A brief overview of intelligent mobility management for future wireless mobile networks

Ilun You^{1*}, Yuh-Shyan Chen², Sherali Zeadally³ and Fei Song⁴

1 Introduction

The increasing number of mobile devices is causing significant changes to applications, networks, and infrastructures. One of the fundamental goals of mobile networks is to enable and support seamless access and handover for current and emerging services. To address the complex challenges of evolving network architectures along with the comprehensive needs of developers and users, novel mobility management techniques and solutions are needed.

With the popularity of new networking technologies such as software-defined network (SDN) and cloud computing, current mobility management protocols and approaches may need to be reevaluated and redefined due to various new issues such as location update, signaling overhead, handover latency, security, and privacy. They could be addressed by intelligent features to increase the performance of mobility management.

After a rigorous and meticulous peer review process, we have selected 21 articles for publication in our special issue. All articles received at least three high-quality reviews. We group the accepted papers according to the relevant topics addressed, and present their proposals briefly below. We hope that this collection of articles provides a useful starting point for further research on intelligent mobility management and technologies in future wireless mobile networks.

2 Mobility models and management techniques

Mobility models and management techniques received a lot of attention in this special issue. In “Modeling link quality for high-speed railway wireless networks based on hidden Markov chain” [1], Song et al. conduct field measurement tests of high-speed railway (HSR) wireless network link quality and they model the link quality using

the hidden Markov chain. They develop an improved algorithm to simulate the variation of HSR wireless network link quality.

In “Interference cancellation for non-orthogonal multiple access used in future wireless mobile networks” [2], X. Su et al. develop an analytical model on error effects of practical successive interference cancellation schemes for non-orthogonal multiple access. The authors further propose an interference-predicted minimum mean square error (IPMMSE) IC by modifying the MMSE weight factor using interference signals.

In “Receiver-assisted cellular/Wi-Fi handover management for efficient multipath multimedia delivery in heterogeneous wireless networks” [3], Cao et al. propose a new receiver-assisted stream control transmission protocol (SCTP)-based cellular/Wi-Fi handover management mechanism for multimedia delivery. The motivation is to (i) optimize SCTP handover management and achieve overhead balancing between the sender and receiver; (ii) improve SCTP loss recovery ability and multimedia transmission performance.

In “A localized fault detection algorithm for mobility management in the strongly t -diagnosable wireless ad hoc network under the comparison model” [4], Kung et al. develop a localized algorithm for detecting faulty nodes in strongly one-step t -diagnosable wireless ad hoc networks (WANETs). They prove that the proposed algorithm only trigger linear time complexity, which is relatively efficient comparing with some other previously proposed schemes in the literature. They also present some examples to clarify how to accomplish the comparison-based fault detection process.

3 Mobility security and privacy protection

Another promising topic is mobility security and privacy protection. In “Global experimental verification of Docker-based secured mVoIP to protect against eavesdropping and DoS attacks” [5], Cha et al. design a prototype of secure mobile VoIP (mVoIP) service with the

* Correspondence: ilsunu@gmail.com

¹Soonchunhyang University, Asan, Choongchungnam-do 31538, Republic of Korea

Full list of author information is available at the end of the article

open-source Asterisk private branch exchange software. The basic elements include Docker lightweight virtualization, secure voice coding and real-time migration technologies.

In “An efficient privacy protection in mobility social network services with novel clustering-based anonymization” [6], Chen et al. propose an approach for categorical data clustering using rough entropy method with DBSCAN algorithm to improve the performance of k -anonymization approach and enhance privacy protection in a mobility social network service.

The article by Gu-Hsin Lai entitled “Detection of wormhole attacks on IPv6 mobility-based wireless sensor network” [7] proposes a RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks)-based wormhole detection mechanism to investigate malicious wormhole nodes if unreasonable rank values are identified.

The article by G. Kim et al. entitled “Secure user authentication based on the trusted platform for mobile devices” [8] describes a TEE-based trusted mobile zone (TMZ) system that builds the trusted platform into mobile devices using virtualization technology. The authors also propose a secure certificate-based user authentication framework using the TMZ system that can increase the reliability of the authentication process performed for multiple devices in mobile networks.

In order to provide an efficient traceable access control in a mobile cloud computing environment, Guan et al., in “An efficient traceable access control scheme with reliable key delegation in mobile cloud computing” [9], construct a traceable CP-ABE system with the access tree and realize the key delegation at servers without loss of traceability and then propose a new type of re-encryption method, which is based on an intuitive method that supports any monotonic access tree.

The article by Nkenyereye et al. entitled “A secure billing protocol over attribute-based encryption in vehicular cloud computing” [10] presents an application model for a secure billing protocol over attribute-based encryption in vehicular cloud computing (VCC). It also proposes a secure billing protocol over attribute-based encryption in VCC based on the techniques of attribute-based encryption, secret sharing scheme, certificateless signature scheme, and hash chain technique.

In “MATF: a multi-attribute trust framework for MANETs” [11], Khan et al. propose a comprehensive multi-attribute trust framework to minimize the bootstrapping time and deal with selective misbehavior. The proposed trust model enhances the security of mobile ad hoc networks by enabling a node to identify and remove malicious nodes from the routing paths by overhearing transmission at multiple nodes. The proposed security scheme not only provides a way to detect attacks and malicious behavior accurately and in a timely way but

also reduces the number of false positives by using the concept of multi-watchdogs.

In “Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network” [12], Gao et al. propose a proxy-based authentication scheme, which combines proxy group signature and identity-based group signature, based on a designated hierarchical proxy architecture, in order to guarantee an efficient anonymous authentication for wireless mesh networks.

4 Mobility prediction and energy efficient mobility

Mobility prediction with big data processing, as well as energy efficient mobility in wireless access networks, has become a key issue in the design of future wireless mobile systems. The article by Sánchez et al. entitled “Predictive algorithms for mobility and device lifecycle management in Cyber-Physical Systems” [13] presents an advance predictive solution for managing the mobility and device lifecycle. The solution can meet all the requirements of cyber-physical systems (CPS). The proposed solution is based on an infinite loop, which calculates, in each iteration, a sequence of future system states using a CPS simulator and interpolation algorithms.

Yang et al., in “Mobility management through access network discovery and selection function for load balancing and power saving in software-defined networking environment” [14], propose an optimal access network discovery and selection function (ANDSF) algorithm for the software-defined networking (SDN) environment. Unlike the traditional ANDSF solution, the proposed algorithm can appropriately assign network resources to user equipment and reduce the power consumption of Wi-Fi access points.

5 Performance analysis of intelligent mobility protocols and architectures

Performance analysis of intelligent mobility protocols and architectures is also an important issue in future wireless mobile networks. In “Secure dissemination of software updates for intelligent mobility in future wireless networks” [15], Lee and Kwon propose a lightweight method to check the integrity of control flow semantics for the Internet of Things (IoT) and mobile environments. The proposed method transforms the binary code of program text into a verifiable form with semantic markers. Thus, it can prove the developers’ intention is unchanged in software update with respect to control flows.

In “Intelligent popularity-aware content caching and retrieving in highway vehicular networks” [16], Quan et al. propose a novel popularity-aware content caching and retrieving strategy in VANETs named P-CCR, which innovatively considers the information-centric networking (ICN) perspective into vehicles’ mobility and vehicular wireless

communication in highway scenarios. The performance analysis shows that the proposed P-CCR solution significantly reduces delay and the number of interest packets, which can reduce network loads and avoid wasting resources.

In “Survivable strategy set design for malicious attack propagation in NEMO scenario” [17], Yao et al. propose two novel survivability strategies to handle malicious attack propagation in network mobility (NEMO) scenarios. The authors use some of the active users to illustrate the NEMO survivability performance based on continuous-time Markov chain and find the relationship between survivability performance and survivable strategy when faced with malicious attacks in a NEMO scenario. The performance analysis results show that it would be helpful for us to choose the right survivable strategy at the right time.

In “Structural analysis of packing schemes for extracting hidden codes in mobile malware” [18], J. Lim and J. Yi analyze the fundamentals behind the main code-hiding schemes used by mobile malware and, through empirical tests, they present methods for extracting the original code hidden in the malware through reverse engineering analysis. The authors also analyze in detail the method of extracting the actual code responsible for malicious behavior from the packed android application package (APK) files.

6 Other issues

There are three articles that deal with other issues related to future wireless and mobile networking technologies. The article by Andrysiak et al. entitled “Network anomaly detection for railway critical infrastructure based on autoregressive fractional integrated moving average” [19] proposes a novel two-stage network traffic anomaly detection method for the railway transportation critical infrastructure monitored using wireless sensor networks.

In “Efficient resource allocation for passive optical fronthaul-based coordinated multipoint transmission” [20], Wang et al. explore both the integer non-linear programming optimization model and the adaptive genetic algorithm to release the capacity pressure of the fronthaul transport network when coordinated multipoint (CoMP) is introduced. The authors also consider the resource allocation problem of the passive optical fronthaul network. Their solution tries to reduce the downlink bandwidth and improve the optical resource allocation efficiency of the optical fronthaul with minimal impact on the fronthaul topology.

In “Mobility support in Named Data Networking: a survey” [21], Feng et al. provide a survey on the mobility support in named data networking (NDN). First, they present the problem statement for both mobile producers and consumers in NDN, and then, they classify

and illustrate mechanisms of existing schemes based on their characteristics. Finally, the authors discuss the advantages and disadvantages of these schemes.

Acknowledgements

We would like to thank the Editor-in-Chief, Prof. Dr.-Ing. Eduard Jorswieck, for providing us with the opportunity to prepare this special issue. We thank all the reviewers for their efforts and for all their valuable and constructive comments which helped us to select the highest quality and most relevant papers for this issue. Finally, we also thank all the authors for their interests and for submitting their works for consideration for publication in this special issue.

Competing interests

The authors declare that they have no competing interests.

Author details

¹Soonchunhyang University, Asan, Choongchungnam-do 31538, Republic of Korea. ²National Taipei University, New Taipei City 23741, Taiwan, Republic of China. ³University of Kentucky, Lexington, KY 40506-0224, USA. ⁴Beijing Jiaotong University, Beijing 100044, People's Republic of China.

Received: 13 October 2017 Accepted: 24 October 2017

Published online: 13 November 2017

References

1. J Song, H Zhou, W Quan, et al., Modeling link quality for high-speed railway wireless networks based on hidden Markov chain. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 263 (2016)
2. X Su, H Yu, W Kim, et al., Interference cancellation for non-orthogonal multiple access used in future wireless mobile networks. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 231 (2016)
3. Y Cao, Q Liu, Y Zuo, et al., Receiver-assisted cellular/wifi handover management for efficient multipath multimedia delivery in heterogeneous wireless networks. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 229 (2016)
4. T Kung, Y Teng, C Lin, et al., A localized fault detection algorithm for mobility management in the strongly t -diagnosable wireless ad hoc network under the comparison model. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 218 (2016)
5. B Cha, J Kim, H Moon, et al., Global experimental verification of Docker-based secured mVoIP to protect against eavesdropping and DoS attacks. *EURASIP J. Wirel. Commun. Netw.* **2017**(1), 63 (2017)
6. Z Chen, H Kang, S Yin, et al., An efficient privacy protection in mobility social network services with novel clustering-based anonymization. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 275 (2016)
7. G Lai, Detection of wormhole attacks on IPv6 mobility-based wireless sensor network. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 274 (2016)
8. G Kim, J Lim, J Kim, Secure user authentication based on the trusted platform for mobile devices. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 233 (2016)
9. Z Guan, J Li, Y Zhang, et al., An efficient traceable access control scheme with reliable key delegation in mobile cloud computing. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 208 (2016)
10. L Nkenyereye, Y Park, K Rhee, A secure billing protocol over attribute-based encryption in vehicular cloud computing. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 196 (2016)
11. M Khan, M Khan, S Malik, et al., MATF: A multi-attribute trust framework for MANETs. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 197 (2016)
12. T Gao, F Peng, N Guo, Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 193 (2016)
13. B Sánchez, R Alcarria, D Rivera, et al., Predictive algorithms for mobility and device lifecycle management in cyber-physical systems. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 228 (2016)
14. S Yang, C Ke, Y Lin, et al., Mobility management through access network discovery and selection function for load balancing and power saving in software-defined networking environment. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 204 (2016)
15. J Lee, T Kwon, Secure dissemination of software updates for intelligent mobility in future wireless networks. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 250 (2016)

16. W Quan, Y Liu, X Jiang, et al., Intelligent popularity-aware content caching and retrieving in highway vehicular networks. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 200 (2016)
17. S Yao, J Guan, H Zhang, Survivable strategy set design for malicious attack propagation in NEMO scenario. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 234 (2016)
18. J Lim, J Yi, Structural analysis of packing schemes for extracting hidden codes in mobile malware. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 221 (2016)
19. T Andrysiak, Ł Saganowski, W Mazurczyk, Network anomaly detection for railway critical infrastructure based on autoregressive fractional integrated moving average. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 245 (2016)
20. G Wang, R Gu, H Li, et al., Efficient resource allocation for passive optical fronthaul-based coordinated multipoint transmission. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 225 (2016)
21. B Feng, H Zhou, Q Xu, Mobility support in named data networking: A survey. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 220 (2016)

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com