Received: 17 April 2018 | Revised: 7 August 2018 | Accepted: 8 August 2018

DOI: 10.1002/itl2.71

LETTER

WILEY

# Peer-assisted location authentication and access control for wireless networks

**Hu Yuan** | **Carsten Maple** | **Yi Lu** | **Tim Watson**

WMG, University of Warwick, Coventry, UK

**Correspondence**
Hu Yuan, WMG, University of Warwick, Coventry CV4 7AL, UK.
Email: h.yuan.4@warwick.ac.uk

**Funding Information**
Engineering and Physical Reseach Council (EPSRC) PETRAS IoT Hub, EP/N02298X/1.

This paper presents the development and implementation of a location-based, lightweight peer-assisted authentication scheme for use in wireless networks. The notion of peer-assisted authentication is based upon some target user equipment-(UE) seeking authentication and access to a network based upon its physical location. The target UE seeks authentication through the UE of peers in the same network. Compared with previous work, the approach in this paper does not rely on any cryptographic proofs from a central authentication infrastructure, thus avoiding complex infrastructure management. However, the peer-assisted authentication consumes network channel resources which will impact on network performance. In this paper, we also present an access control algorithm for balancing the location authentication, network quality of service (QoS), network capacity and time delay. The results demonstrate that peer-assisted authentication considering location authentication and system QoS through dynamic access control strategies can be effectively and efficiently implemented in a number of use cases.

**KEYWORDS**

access control, location authentication, quality of service, wireless networks

## 1 | INTRODUCTION

Driven by the proliferation of Wi-Fi hotspots and femtocells in public places, location-based services (LBSs) have experienced a surge in development in recent years.[1] In LBS systems, users can request a location-dependent service from LBS providers. However, to ensure appropriate use, and assist in the security, of these services, authentication is important. Once mobile users are authenticated, it is possible to grant specific access permissions, such as multimedia-based tourism and nearby marketing.

### 1.1 | Related work

There has been increased interest in LBS systems recently. To identify the location of a mobile user, one of the main methods employed is based on the visiting history of user equipments (UEs). By analyzing frequently visited locations of users in the past 6 months, for example, the validation of the current access location can be judged and a digital signature can be provided based on the result.[2] Similarly, in Reference,[3] the BSSID (Wi-Fi MAC address) and RSSI (recovered Wi-Fi signal strength) are recorded while users log into Wi-Fi access points. This location profile is leveraged to generate an authentication questionnaire. The questions concern information about the user's location, such as recently visited places and the order they visited.

However, using such a location authentication architecture, a trusted infrastructure is required to achieve a relatively high degree of confidence by using cryptographic protocols. This necessarily increases the complexity of authentication. In this paper, we present a peer-to-peer authentication system which does not require a central infrastructure but is still able to provide efficient authentication.

The authentication approach in this paper is based on the *trusted* locations of network utilities (such as cellular femtocells or Wi-Fi Access point [APs]),[4,5] and those utilities can be used to prove the location of nearby mobile devices. This overcomes the requirements in previous work such as certification authorities,[6] cryptographic location proofs,[7] or trusted platform modules.[8]

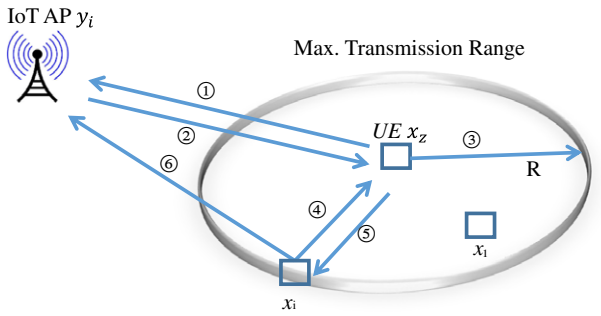


**FIGURE 1** Illustration of assistance authentication in the Internet of Things (IoT)

### 1.2 | Contribution and organization

Our proposed approach overcomes previous limitations by authenticating the location of what we term target UEs, through the use of peer UE within the coverage area of the relevant AP. Our key contributions include: (1) A lightweight, noncryptographic method of using cooperating users to verify an entrusted user's location. (2) An access control method that balances the strength of authentication and network QoS. This is needed since a network with a high volume of UEs, will have network resources that are tightly constrained. However, it must be noted that the peer UEs occupy the communication channel while they are authenticating the target UE's location.

The remainder of this paper is organized as follows. The system model is presented in Section 2, and the authentication probability success based on the peer-assisted authentication is considered in Section 3 . In Section 4, the network QoS (eg, network capacity and time delay) is analyzed and a related access control method is introduced. The numerical results of the success authentication probability are analyzed in Section 5 before Section 6 presents the results and ongoing challenges.

## 2 | SYSTEM MODEL

The system considered in this paper is a heterogeneous wireless Internet of Things (IoT) network. It contains a range of mobile IoT (MIoT) technologies standardized by the third Generation Partnership Project (3GPP).[9] As shown in Figure 1, IoT UEs (from $x_1$ to $x_i$) access the IoT services through the IoT AP $y_i$. When a new user $x_z$ wants to join the network, a peer-assisted location authentication scheme is employed. The scheme uses the existing UEs within the network to assist authenticating the target UE for LBS. It does not use a transitional mutual authentication with UEs through the evolved packet system Authentication and Key Agreement protocol.[10]

For the analysis, the assumptions in this paper are as follows: (1) The UEs within the existing cellular network are secured and authenticated; (2) The probability of UEs ($x_i$) willing to assist the new UEs is modeled as a probability $P$ valued by a Normal distribution; iii) The traffic model is assumed to be a full buffer and the relaying protocol used is a time division duplex (TDD) network. The authentication success probability is defined as at least one UE being willing to assist.

### 2.1 | Peer assistance authentication

As shown in Figure 1, when UE $x_z$ requests a LBS and UE $x_i$ is used for peer-assisted location authentication of UE $x_z$. The operation details are:

1. The UE $x_z$ sends an internet accesses request to IoT network AP. This includes the service type and QoS requirement (network capacity and time delay);
2. AP returns the authentication information identity frame $D$, which is a data frame containing the channel state information (CSI). Once $x_z$ received frame $D$, it executes the authentication scheme;
3. The UE $x_z$ broadcasts an assistance signal to other UEs. If $x_i$ is within the transmission range of $x_z$, and is willing to help then it replies with an acknowledgment;
4. $x_z$ updates and sends the authentication information package $D$ to the UE $x_i$;
5. $x_i$ updates and relays the data $D$ to the AP for verification.
6. When the AP receives the data frame $D$, it compares the CSI of authentication participators for verifying the location of $x_z$.

## 3 | SUCCESSFUL AUTHENTICATION PROBABILITY

We assume the probabilities $P_i$ are independent and identically distributed. So the successful authentication probability is $\mathbb{P} = 1 - \prod_{i=1}^{N}(1 - P_i)$, where $N$ is the total number of assisting UEs.

### 3.1 | IoT UE distribution

A doubly Poisson cluster process is used for generating the UE distribution. The UEs are uniformly scattered on the circle centered at each AP. The APs $y_j$ are deployed using Poisson point processes (PPP) $\Phi_{\text{AP}} = \{y_1, y_2, \ldots, y_j, \ldots\}$ with constant density $\Lambda_{\text{AP}}$. The UEs are deployed from another PPP $\Phi_{\text{UE}} = \{x_1, x_2, \ldots, x_i, \ldots\}$ with the UE density $\Lambda_{\text{UE}}$. The UE clusters are $\mathfrak{N}_{x_i} = \mathfrak{N} + y_i$ for each $y_i \in \Phi_{\text{AP}}$ and random point process $\mathfrak{N}$ . The whole process of $\Phi_{\text{UE}}$ is $\Phi_{\text{UE}} = \bigcup_{y \in \Phi_{\text{AP}}} \mathfrak{N}_x$.

For any subset of a Euclidean space $\mathscr{B}$, $N(\mathscr{B})$ is the number of points in the set $\mathscr{B}$, the number $N(\mathscr{B})$ has a Poisson distribution with the density $\Lambda_{UE}$ of a space set of $\mathscr{B}$. Therefore the probability of $k$ random Poisson points in the set $\mathscr{B}$ is[11]:

$$\mathbb{P}(N(\mathscr{B})=k)=\exp\left(-\int_{\mathscr{B}}\Lambda(x)\mathrm{d}x\right)\frac{\left(\int_{\mathscr{B}}\Lambda(x)\mathrm{d}x\right)^{k}}{k!}, \tag{1}$$

where $\int_{\mathscr{B}}\Lambda(x)\mathrm{d}x=A\Lambda_{UE}$, and $A$ is the area of the space $\mathscr{B}$.

So the probability of the number of random points in the two-dimensional set $\mathscr{B}$ is,

$$\mathbb{P}(N(\mathscr{B})=k)=\exp(-\Lambda_{UE}A)\frac{(\Lambda_{UE}A)^{k}}{k!}. \tag{2}$$

### 3.2 | The number of assisting UEs

In order to characterize the performance of successful authentication probability, it is necessary to determine the number of UEs participating in the peer-assisted authentication. This number depends on the UE density and maximum transmission range of UEs. As shown in Figure 1, each UE is capable of transmitting a signal of up to a distance of $R$. For the requirement of the data communication, the required minimum signal-noise-ratio (SNR) $\gamma$ is $\zeta$. The maximum transmission distance is defined such that the SNR of the receiver is bigger than the SNR threshold $\zeta$.

$$R=\arg\max\{\gamma\geq\zeta\}=\arg\max\left\{\frac{HP_{UE}\lambda_{UE}r^{-\alpha}}{\sigma^{2}}\geq\zeta\right\}, \tag{3}$$

where $H$ is the channel fading gain, $P_{UE}$ is the transmission power of UEs, $\lambda_{UE}$ is the frequency-dependent pathloss constant, $\alpha$ is the pathloss distance exponent, $r$ is the distance between the transmitter and receiver UEs and $\sigma^2$ is the additive white Gaussian noise. Without considering the multichannel gain, the maximum transmission distance is:

$$R=\left(\frac{P_{UE}\lambda_{UE}}{\sigma^{2}\zeta}\right)^{-\frac{1}{\alpha}}. \tag{4}$$

The probability of the number of random points is shown in Equation (2), by applying Equation (4) the expectation of assisting UEs within the maximum transmission range $R$ is given by:

$$\begin{aligned}\mathbb{E}(N)&=\sum_{k=0}^{k=+\infty}k\exp(-\Lambda_{UE}A)\frac{(\Lambda_{UE}A)^{k}}{k!}=\exp(-\Lambda_{UE}\pi R^{2})\sum_{k=1}^{k=+\infty}\frac{(\Lambda_{UE}\pi R^{2})^{k}}{(k-1)!}\\&=\exp\left[-\Lambda_{UE}\pi\left(\frac{P_{UE}\lambda_{UE}}{\sigma^{2}\zeta}\right)^{-\frac{2}{\alpha}}\right]\sum_{k=1}^{k=+\infty}\frac{\left[\Lambda_{UE}\pi\left(\frac{P_{UE}\lambda_{UE}}{\sigma^{2}\zeta}\right)^{-\frac{2}{\alpha}}\right]^{k}}{(k-1)!},\end{aligned} \tag{5}$$

Applying Equation (5), the successful authentication probability is:

$$\mathbb{P}=1-\prod_{i=1}^{\lceil\mathbb{E}(N)\rceil}(1-P_{i}). \tag{6}$$

where $\lceil\mathbb{E}(N)\rceil$ is rounded up.

## 4 | NETWORK PERFORMANCE AND ACCESS CONTROL

Quality of Service (QoS) is a particularly important parameter for network performance. This is because network resources such as frequency bandwidth and available time slots are limited. In this section, the network capacity and time delay under the assisted authentication scheme are addressed.

During the peer-assisted authentication process, UEs are broadcasting both request signals and Acknowledgments (ACKs). Thus they would consume channel resources such as frequency bandwidth for the frequency division duplex (FDD) channel or available time slots for the TDD channel. Network performance is highly dependent on the channel resources available. We propose an access control protocol for managing LBS dependent on the network QoS and authentication requirement.

### 4.1 | IoT UEs capacity

The first index is capacity, from the Shannon theory, the network capacity related to SNR is $C=B\log_2(1+\gamma_i)$ where $B$ is the channel bandwidth. The expectation of a nonnegative continuous random variable $X$ is $\mathbb{E}[X]=\int_{t>0}\mathbb{P}(X>t)\mathrm{d}t$. Therefore, expectation capacity of a single IoT UE is:

$$\mathbb{E}(C_{i})=\int_{0}^{+\infty}\mathbb{P}\left\{B\log_{2}\left[1+\frac{HP_{AP}\lambda r^{-\alpha}}{\sigma^{2}}\right]>\zeta\right\}\mathrm{d}\zeta, \tag{7}$$

The multipath fading has a pdf of $f_H(h)\sim\exp(\beta)$, where $\beta=1/P_{AP}\lambda$.

By a known spatial distribution of UEs, the definition of the mean capacity of the channel is given by:

$$\overline{C}=\int_{0}^{+\infty}\mathbb{E}(C_{i})f_{R}(r)\mathrm{d}r=\int_{0}^{1}-e^{\mathscr{A}(y,\alpha)\sigma^{2}}\frac{B}{\mathscr{A}(y,\alpha)\sigma^{2}\ln 2}\Gamma(0,\mathscr{A}(y\alpha)\sigma^{2})\mathrm{d}y, \tag{8}$$

where $\mathscr{A}(y, \alpha)$ is given as[12]:

$$\mathscr{A}(y, \alpha) = \beta\left(\sqrt{\frac{\ln y}{-\Lambda_{\mathrm{AP}}\pi}}\right)^{-\alpha}, \quad 0 \le y \le 1. \tag{9}$$

## 4.2 | Average time delay

Let $P_{k(k+1)}(t)$ be the probability that given the process $X$ is in state $k$ at time $t_0$, then at a time $t$ later, it will be in state $k+1$. This process can be modeled as[13]:

$$P_{k(k+1)}(t) = P[X(t_0 + t) = (k+1) | X(t_0) = k], \tag{10}$$

The steady-state probabilities are defined as, $\varphi_{k+1} = \lim_{t\to\infty} P_{k(k+1)}(t)$ where $\varphi_{k+1}$ is the steady-state probability at state $k+1$. The global balance steady-state equations for the $M/M/1/K$ is obtained: $\varphi_k \tau = \varphi_{k+1}\mu$ for $k = 0, 1, 2, 3, ..., K-1$ where $K \ge 1$, $K$ is the size of the system buffer. The normalizing equation is $\sum_{k=0}^{K} \varphi_k = 1$.

Therefore, the probability that there is no UE in the IoT system is,

$$\varphi_0 = \frac{1}{1 + \sum_{k=1}^{K}\left(\frac{SN_{\mathrm{Wi-Fi}}}{\overline{C}\sum_{i=0}^{N_{\mathrm{IoT}}} T_i}\right)^k} = \begin{cases} \frac{1-\rho^{K+1}}{1-\rho} & \rho \ne 1 \\ \frac{1}{K+1} & \rho = 1, \end{cases} \tag{11}$$

where $\rho = \frac{SN_{\mathrm{IoT}}}{\overline{C}\sum_{i=0}^{N_{\mathrm{IoT}}} T_i}$, $S$ is the transmission data size, $N$ is the number of assistant UEs and $\overline{C}$ is from Equation (8). The IoT traffic confliction probability is the probability that at least one UE is communicating in the system.

$$P_{\mathrm{c}} = P\{\text{at least one UE}\} = \begin{cases} 1 - \frac{1-\rho^{K+1}}{1-\rho} & \rho \ne 1 \\ 1 - \frac{1}{K+1} & \rho = 1. \end{cases} \tag{12}$$

The communication system is a TDD system, so only one UE can transmit at any one time. Therefore, the average time delay is:

$$\mathbb{E}(T_D) = \mathbb{E}(T_W) + \mathbb{E}(T_{Sr}), \tag{13}$$

where $\mathbb{E}(T_W)$ is the mean data transmission time and $\mathbb{E}(T_{Sr})$ is the mean system severing time, $S/\overline{C}$ in the IoT system.

The system limit is $K$, so when $K$ UEs are in the system there is no access for the next UE. Therefore, the mean waiting time is given by:

$$\mathbb{E}(T_W) = \begin{cases} \left[\frac{\rho}{1-\rho} - \frac{(K+1)\rho^{K+1}}{1-\rho^{K+1}}\right]\frac{1}{\tau(1-\rho^K\varphi_0)} & \rho \ne 1 \\ \frac{K}{2\tau(1-\rho^K\varphi_0)} & \rho = 1. \end{cases} \tag{14}$$

## 4.3 | Access control algorithm

**Algorithm 1** Access Control Algorithm

1: **function** IoT ACCESS($P_i$, $\alpha$, $S$, $\Lambda_{\mathrm{AP}}$, $\Lambda_{\mathrm{UE}}$)
2: *The defined parameters of LBS access required UE: success authentication $P'$, delay $T'$, and capacity $C'$*
3: *Calculate* probability $\mathbb{P}(P_i, \alpha, \Lambda_{\mathrm{UE}})$ from Equation (6)
4: **if** ($\mathbb{P} \le P'$) **then** *LBS access declined*
5: **else** ($\mathbb{P} \ldots P'$)
6: *Calculate capacity $\overline{C}(\alpha, \Lambda_{\mathrm{AP}})$ from Equation (8)*
7: *Calculate delay $\mathbb{E}(T_D)\{\alpha, \Lambda_{\mathrm{AP}}, S\}$ from Equation (13)*
8: **if** $\overline{C} > C'$ç$\mathbb{E}(T_D) > T'$ **then**
9: *LBS access allowed*
10: **else**
11: *LBS access put on waiting list*
12: **end if**

According to the QoS and authentication requirements, an access control algorithm is executed. When a new LBS call arrives: (1) If the authentication level is not satisfied based on the peer-assisted authentication, the service call is declined. (2) If the authentication level is satisfied then the scheme checks the QoS (capacity, delay) in the system. (i) If the QoS quality is met, the service call will be processed. (ii) If there is not enough network capacity or the delay is bigger than requested, when a new call arrives the call will be put on the waiting list. The processing of the algorithm is shown in Algorithm 1.

# 5 | NUMERICAL RESULTS AND ANALYSIS

In this section, the simulation results are presented to analyze the performance of IoT communication systems with assistance authentication protocols. In this paper, channel bandwidth is 20 MHz, AWGN Power $\sigma$ is $-162$ dB, AP Transmit Power $P_{\mathrm{AP}}$ is 40 W, IoT UE Transmit Power $P_{\mathrm{UE}}$ is 1 W, D2D UE Density

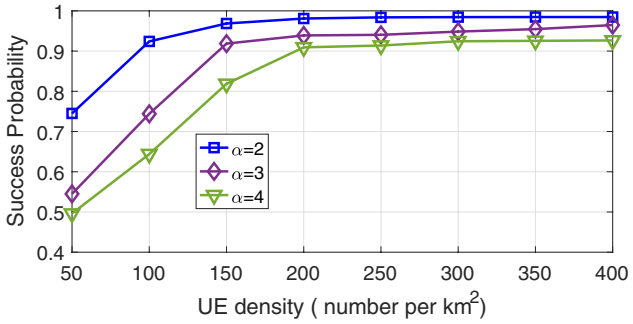


**FIGURE 2** The probability of successful authentication with user equipments (UEs) density compared with different $\alpha$

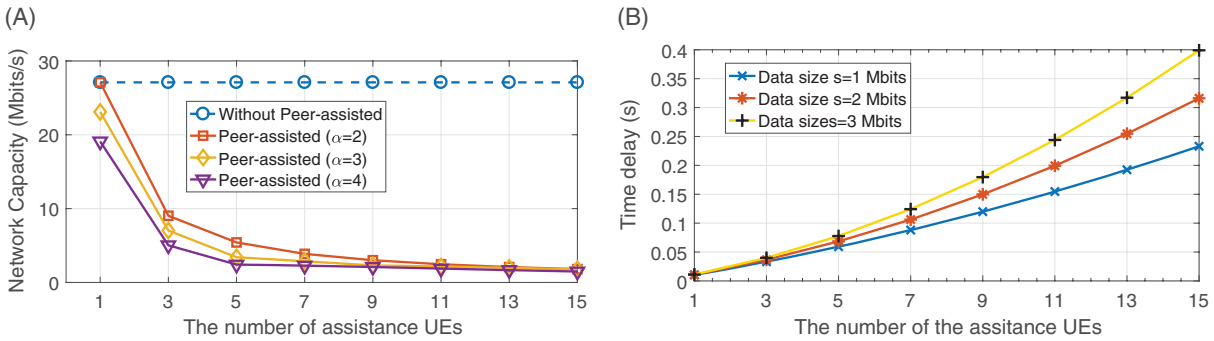


**FIGURE 3** The network performance with different number of peer-assisted authentication UEs. A, Network capacity with different $\alpha$. B, Package delay with different traffic conditions

$\Lambda$ is 50 to 400 km$^2$ and the data communication threshold SNR is $-6$ dB. The IoT network radius is 500 m with eight APs providing the IoT access. The system severing time is $\tau = 0.05$ seconds. Three different IoT traffic volumes are selected to analyze the performance: light traffic with data package size 1000 kbits; medium traffic with data package size 2000 kbits, and heavy traffic with data package size 3000 kbits. The pathloss distance exponents are 2, 3, and 4 representing different communication environments: suburban, rural, and dense urban, respectively.

## 5.1 | Successful authentication probability

From the results shown in Figure 2, the assisted authentication can achieve an acceptable successful authentication level. The successful authentication probability would climb to 75% with user density 50 or even to 97% with user density 400 where $\alpha$ is 2. When the pathloss distance exponent increases from 2 to 4, the successful authentication probability decreases. Because the transmission range is decreasing, the number of available assistance UEs is less. When there are fewer UEs the successful authentication probability decreases.

The user density has a significant effect on success of peer-assisted authentication. As such the peer-assisted authentication is suitable for high UE density scenarios, such as multimedia tourism services, where the LBS can deliver the scenic spot location, city history, and traffic information-based locations of visitors. However, for a low UE density environment, such as a rural area, the peer-assisted authentication does not work efficiently. Under this situation, a different location authentication scheme is needed.

## 5.2 | Network performance with peer-assisted authentication

As Figure 3A shows, without the peer-assisted authentication the network capacity is 27.1 Mbits/s but with assistance, the network capacity is reduced to 1.8 Mbits/s when the number of assistance UEs is over 13. The different values of $\alpha$ show the same tendency.

Thus peer-assisted authentication is suitable for applications requiring lower capacity. However, for some high capacity network applications such as live video or online games, the peer-assisted authentication would seriously reduce the network performance.

When the assistance authentication is utilized, the IoT UEs have to wait a period for the UE identification. Figure 3B shows the average time delay of the different number of assistance UEs compared with different network traffic volumes. The delay time would climb from 0.01 to 0.4 seconds with a data package size of 3000 kbits. The system average time delay increases significantly when more UEs take part in the authentication. The impact is greater with bigger data sizes.

In this paper, a TDD network is considered for analysis. For an FDD network, the same tendency would be observed since the assisted UEs cause interference with other UEs. The interference leads to a greater bit error rate (BER) and reduces channel capacity.

## 5.3 | Under QoS requirement constraint

Figure 4 displays a qualitative comparison of different QoS and authentication requirement. Generally, the more UEs participating in peer-assisted authentication, the bigger the impact on the network performance. Specifically, for a relatively low QoS requirement (such as 0.4 s delay and 1 Mbits/s), more

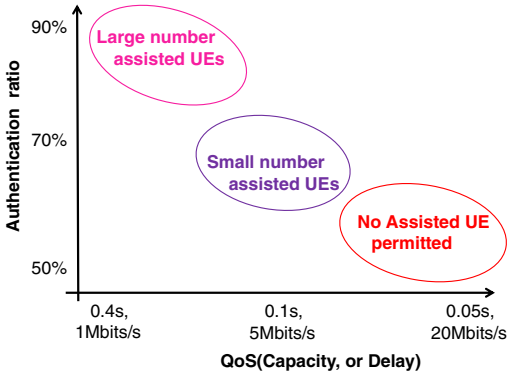


**FIGURE 4** The balance in assistance authentication operations between network security and system quality of service (QoS)

UEs are allowed for assisted authentication. Conversely, when the requirement changes to 0.05 seconds and 20 Mbits/s, no UEs are allowed for assisted authentication.

## 6 | CONCLUSION AND FURTHER WORK

In this paper, a novel lightweight and noncryptographic location authentication scheme, which relies on decentralized peer to peer-assisted authentication, is implemented for wireless networks. The peer-assisted authentication can achieve a relatively high successful authentication probability. While UEs assist the AP to authenticate the target UE's location, they occupy the channel resources. Thus, the network performance (channel capacity, time delay) is reduced, a QoS-based access control is executed to balance the network performance and authentication.

The security and privacy become big challenges in LBS applications.[14] In our approach, the location privacy of assisted UEs is leaked to the target UE. Thus, our further work will be based on privacy aware LBS.[15]

### ACKNOWLEDGMENTS

This work has been supported by the EPSRC project PETRAS IoT Hub (EP/N02298X/1).

### ORCID

*Hu Yuan* http://orcid.org/0000-0001-9833-5930

### REFERENCES

1. Ryschka S, Murawski M, Bick M. Location-based services. *Bus Inf Syst Eng*. 2016;*58*(3):233-237.
2. Hongyan Z, Jinchun G, Yuan'an L, Xiaolei M. A digital signature with high security based on location information. Paper presented at: IEEE International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC); 2013; Shengyang, China:2607–2611.
3. Albayram Y, Khan MMH, Bamis A, Kentros S, Nguyen N, Jiang R. A location-based authentication system leveraging smartphones. Paper presented at: IEEE 15th International Conference on Mobile Data Management (MDM); 2014; Brisbane, Australia:83–88.
4. Saroiu S, Wolman A. Enabling new mobile applications with location proofs. Paper presented at: ACM The 10th Workshop on Mobile Computing Systems and Applications; 2009; California.
5. Aloudat A, Michael K, Chen X, Al-Debei MM. Social acceptance of location-based mobile government services for emergency management. *Telematics Inform*. 2014;*31*(1):153-171.
6. Wang W, Chen Y, Zhang Q. Privacy-preserving location authentication in Wi-fi networks using fine-grained physical layer signatures. *IEEE Trans Wirel Commun*. 2016;*15*(2):1218-1225.
7. Magkos E. Cryptographic approaches for privacy preservation in location-based services: A survey. Paper presented at: IGI Global 2012; Greece; 2012:273–297.
8. Gilbert P, Cox LP, Jung J, Wetherall D. Toward trustworthy mobile sensing. Paper presented at: ACM Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications; 2010; Annapolis, MD:31–36.
9. Takehiro N, Satoshi N, Anass B, et al. Trends in small cell enhancements in LTE advanced. *IEEE Commun Mag*. 2013;*51*(2):98-105.
10. Muxiang Z, Yuguang F. Security analysis and enhancements of 3GPP authentication and key agreement protocol. *IEEE Trans Wirel Commun*. 2005;*4*(2):734-742.
11. Andrews JG, Francois B, Krishna GR. A tractable approach to coverage and rate in cellular networks. *IEEE Trans Commun*. 2011;*59*(11):3122-3134.
12. Yuan H, Guo W, Jin Y, Wang S, Ni M. Interference-aware multi-hop path selection for device-to-device communications in a cellular interference environment. *IET Commun*. 2017;*11*(11):1741-1750.
13. Bose SK. *An Introduction to Queueing Systems*. New York, US: Springer Science & Business Media; 2013.
14. Maple C. Security and privacy in the internet of things. *J Cyber Policy*. 2017;*2*(2):155-184.
15. He X, Jin R, Dai H. Leveraging spatial diversity for privacy-aware location-based services in mobile networks. *IEEE Trans Inf Forensic Secur*. 2018;*13*(6):1524-1534.

**How to cite this article:** Yuan H, Maple C, Lu Y, Watson T. Peer-assisted location authentication and access control for wireless networks. *Internet Technology Letters* 2018;e71. https://doi.org/10.1002/itl2.71