DESIGN OF LOCATION BASED AUTHENTICATION SYSTEM USING VISIBLE LIGHT COMMUNICATION

[1]KHAIRUL AZMI ABU BAKAR, [2]DAHLILA PUTRI DAHNIL

[1,2]Research Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia,43600 Bangi, Malaysia

E-mail: [1]khairul.azmi@ukm.edu.my, [2]dahlila@ukm.edu.my

ABSTRACT

User location information provides additional layer of security to a system. The location information of a user is an important attribute that can be used in authentication systems. Legitimate user has to be physically resides within a restricted area to gain access. With the growth of wireless communication technologies that use radio waves, determination of user location for indoor environment is very challenging. Radio signal can penetrate walls; thus it is not easy to verify location information within a restricted area as small as a room. In this paper, we propose a location-based authentication system that is cost-effective and user friendly. The proposed system uses common infrastructure such as LED lightbulb and smartphone. To verify the location of the user, visible light communication technology via the LED lightbulb is used.

Keywords: *VLC, Location Based System, User Authentication, QR Code, Security*

1. INTRODUCTION

Authentication is an important component in information system security. User~~s~~ who wish to access confidential resources in the system need to have his identity verified. Authentication provides a mechanism to verify the identity of users by requesting the intended user to provide credential or authentication method. Those who can successfully present the valid credential are considered as authenticated user. Only authenticated users with the proper authorization would be allowed to access the resources.

In general credentials used in authentication process can be categories into three groups of factors as the following:

a. What you know - knowledge of some shared secret (password, PIN, etc.)

b. What you have - possession of something given to the user (smartcard, token, etc.)

c. What you are - either physical (fingerprint, retina, etc.) or behavioral characteristic of a user (typing patterns, habitual behavior, etc.)

Each of the factors has its own advantages and disadvantages. The "*what you know*" factor is convenient and does not bear any maintenance cost for the users and the system. However, this factor is vulnerable to shoulder surfing attack. The users also have to always remember the shared secret to get authenticated. To preserve the security level of the system, the chosen shared secret should be complex which makes it very difficult for the actual user to remember.

The "*what you have*" factor on the other hand does not require user~~s~~ to remember as the user only need to present a physical object as ~~a~~ prove of identity. However, this solution bears some cost to purchase the object used as the credential. The users must always have the object in possession to get authenticated. This type of factor could create problem if the object used as the credential is misplaced or lost. The object might also be stolen by attacker who will be able to impersonate the owner of the object.

The "*what you are*" factor seems to offer a solution to the problems from the previous factors. User does not have to remember a secret key or carry an object to get authenticated. Unfortunately, biometric sensors are fairly expensive and at many time are not accurate. Furthermore, if the user biological traits are copied and duplicated, it is almost impossible for the user to change or replace the credential.

In order to complement the disadvantages in each of the factor, most authentication systems implement multi factor authentication (MFA). Multifactor authentication is a security system that requires more than one credential from independent groups of factors to verify user's identity. One typical example is the ATM (Automated Teller Machine). Before the bank customer is allowed to perform banking transactions, ATM machines require the customer to present his personal bankcard (something you have) and enter his Personal Identification Number (something you know). However, if the adversary has access to those two factors, the ATM machine will still consider the adversary as the authenticated user.

Location based authentication adds a strong new layer to information security by allowing organization to ensure that only authorized users from a predetermined area have access to confidential resources. In some highly secure environment such as in the military, healthcare and government agencies, access to confidential data might be restricted to a room or a set of room [1]. This restriction makes it harder for any adversary to attack the system as they have to be located within the parameter. Nevertheless, controlling access of data based on location is not only complicated but expensive to implement and maintain [2].

There are many existing technologies to determine the location of the user. The most common technology is by using Global Positioning System (GPS). GPS uses a constellation of four or more earth orbit satellites that continuously transmit messages using radio signals. GPS receivers measure the transmit time of each messages and compute the distance to each satellites. A form of triangulation is used to combine these distances with the location of the satellites to determine the receiver's location with the accuracy of around 3 meters. However, GPS receivers require an unobstructed line of sight to the earth satellites. GPS signal could not pass through solid structures. As a result, GPS technology is not suitable to be used indoor, underground, under the water or under a dense canopy of trees.

Another method to determine the location of the user is by simply referring to the IP Address of the user's machine. There are number of free and paid subscription geolocation databases than can identify the real-world geographic location of the machine based on its IP Address. URL sites such as [3-6] provides geolocation information ranging from country level to state or city, each with varying claim of accuracy. However, this method could not be used to identify a small area zone such as a room or hall. In addition, geographical location implementation with this method does not work if the user accessing the system through proxy or VPN (Virtual Private Network) server. In that case, the user will be detected bearing IP address of the proxy or VPN server.

Wireless communication has become a popular medium for data communication. Wireless communication allows user to freely move around without having to worry about the trailing cables and still get connected to the network. Besides those advantages of wireless communication, it also presents a big challenge to determine user location. Wireless communication uses radio signals that could penetrate walls and building. Depending on the wireless communication technology used, the signal travelling distance could be ranging from 100 meters (Wi-Fi) to several kilometers (4G). As a result, current wireless technology is not suitable to be used for location based authentication.

This paper proposes a user-friendly authentication system that requires location information as an input parameter to validate the identity of the user. In other words, the user has to be positioned within an authorized area to gain access to the system. First, beacon messages from a personalized transmitter are broadcast. Special care need to be taken as to confine the beacon message not to exceed the dedicated area. User's personalized smart phone needs to be located within that authorized area in order to capture the beacon message and generate a time-based QR Code. Both personalized transmitter and smart phone have unique secret keys stored which are used as inputs to generate the QR Code. The QR Code is then scanned by the user's computer via the web cam and send to the server to be validated.

The remaining of the paper is organized as follows: The proposed location based authentication system that is able to comply the stated requirements is introduced in Section 2. Section 3 discusses about the justification in several aspects when making decision around the idea of the proposed system. Related works with regards to the proposed system are briefly reviewed in Section 4. Finally, the conclusion of this paper is given in Section 5.

2. PROPOSAL

In this paper we are proposing a solution that would allow system administrator to implement location based security policy that satisfy the following requirements:

a. The system can be used for indoor environment

b. The size of the authorized area for the user to gain access is as small as a standard office room

c. The system should be transparent. User should not be aware of the installed system.

d. The user should not bear any additional cost to use the system

e. The system should have low maintaining cost

The proposed solution makes use of Visible Light Communication (VLC) technology. VLC is a type of data communication which uses the spectrum of visible light as the data transmission medium. VLC sends data signal by modulating the intensity of the existing Light Emitting Diodes (LED) lightbulb on and off extremely quick to be detected by the human eye.

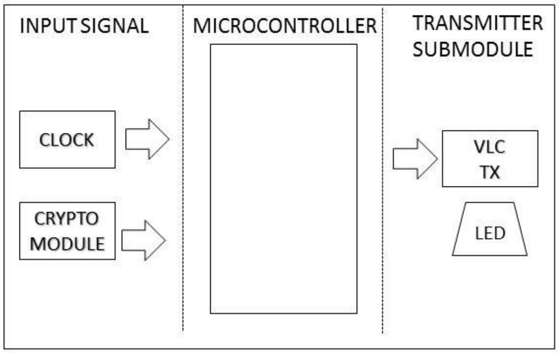

Figure 1. VLC Transmitter

The use of VLC in the solution can be described into two parts: Transmitter and Receiver. Figure 1 depicts a block diagram of a VLC transmitter. There are three components of a VLC transmitter: Input data, microcontroller and transmitter submodule. Input data consists of two input signals: clock and crypto module. The clock module provides the real time clock data to the microcontroller. Crypto module on the other hand stores a unique shared secret key assigned to the VLC transmitter. Microcontroller uses these two input signals to generate series of digital beacon messages that changes every minutes. The series of digital beacon messages are then send to the transmitter submodule which translates the messages by switching on and off the connected LED lightbulb. The basic rule is bit 1 for light on and bit 0 for light off.

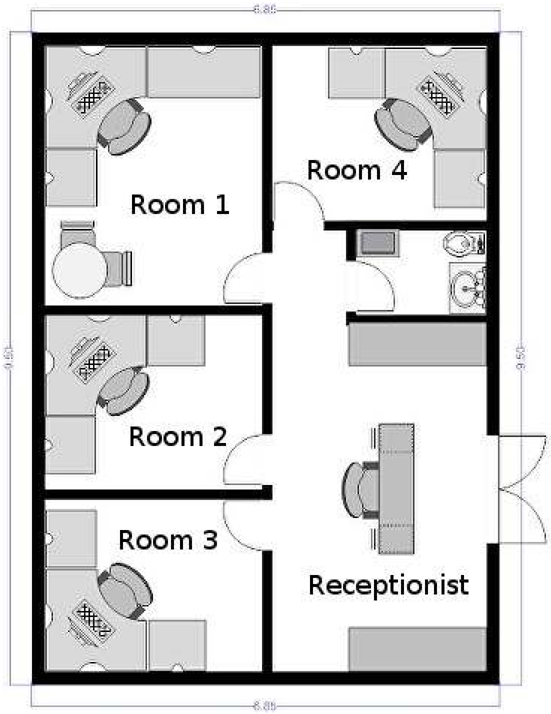

Figure 2. Office Layout

Figure 2 illustrates a sample layout for a normal office building. In this setup there are four rooms in the office. Each room is installed with a VLC transmitter which is used for lightning purpose and also for transmitting beacon messages. Each of the transmitters has a crypto module which has been stored with a unique shared secret key. At any time, each of the transmitters would broadcast different time-based key. The wall of the room is made of a solid material so that the light from one room does not leave to the neighboring room.

A VLC receiver is constructed from a photosensitive detector which in this case a standard camera on the smartphone. The smartphone can be either an Android or iPhone and must be personalized to the user as it is used as a prove identity of the user. The smartphone should be installed with an application that would be able to capture beacon messages from the VLC transmitter via the camera and generate QR Code based on the message and time factor.

Another equipment used in this solution is the computer which can be a laptop or a desktop equipped with a web cam. Currently most of the laptop computers have built in web cam installed. The computer should also have been installed with a browser that is able to run javascript and support

HTML5. HTML5 is a new upcoming standard for content structure and presentation on the World Wide Web. One of the new features introduced with HTML5 is the ability for the browser to access multimedia stream (video, audio or both) from local devices. HTML5 specifies getUserMedia API (Application Programming Interface) which allows access to the web cam from the browser with a single function call without requiring any installation of additional software. This feature is now supported by many latest version of popular browsers such as Firefox, Mozilla, Opera and Chrome.

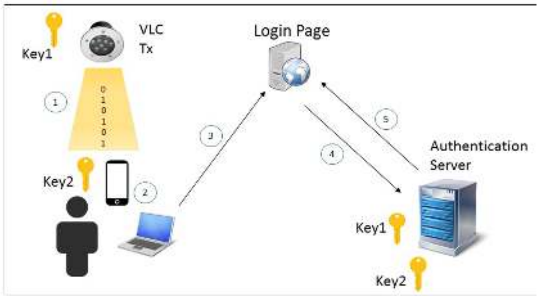

Figure 3. Process Flow

Figure 3 illustrates the overall process flow of the proposed system. When a user browses the protected website, a login page will be displayed. The user needs to run the mobile application on the smartphone. The application is responsible to perform two tasks. First is to generate a time factor crypto key based on the installed symmetric key and the time. Second, the application would activate the camera of the smartphone and capture the beacon message from the VLC transmitter inside the room. By convention, light on means logical 1 and light off means logical 0. By using both data (crypto key and the VLC message separated by a character '|'), the application generates a QR Code as shown in Figure 4.

When the user clicks to the smartphone icon at the login page, the browser executes a javascript which then triggers HTML5 API to gain access to the local webcam. The browser may prompt the user asking for the permission. Once the permission is granted, the webcam will start looking for the QR Code. User needs to point the generated QR Code from the smartphone to the webcam. The browser then extracts the key from the QR Code and send the key to the server to be verified.

The server looks for two things. First is to verify that the user has presented a valid authentication method which in this case the user personalized smartphone. Second is to confirm whether the user is logging from the authorized area which is indicated from the beacon message from the VLC transmitter. The server is able to perform the verification for both cases since it has both keys. Only if both conditions are met, the user will be authenticated by the system.

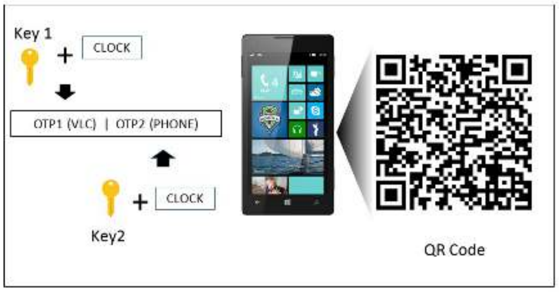

Figure 4. QR Code Generation

3. DISCUSSION

There are several aspects that were put into consideration when making decision around the idea of the proposed system. First is the decision to use the smartphone as the main user credential. Smartphone has no longer a luxury item but has become a universal accessory device owned by enormous number of people worldwide. According to the statistic released by United Nations' International Telecommunication Union, there are more than 7 billion mobile cellular subscriptions by end of 2015 around the globe, up from 738 million in 2000 [7]. That corresponding to a penetration rate of 97%.

One major reason smartphone is chosen as the credential is because of its current status as a personal belonging. Smartphone has achieved a status on par with wallets and keys where they are always carried when leaving the home. Users are keen to use their smartphone to store personal information such as email addresses and phone numbers from the contacts, calendar appointments, personal photos and videos. Because of this trend, users are very concern if their smartphones are missing or lost. According to a survey conducted by YouGov on behalf of SecurEnvoy, a third of smartphone owner would realize they had lost their smartphone within 15 minutes [8]. The study which was done to 2,000 smartphone owners also claim that a majority would probably notice about the smartphone missing within an hour.

Smartphone increase the safety of the device as they have their own security system. Depending on the security settings used, the screen on the smartphone will be locked after an inactive period. To unlock the screen, the user has to present the required credential. Many of the current smartphones support multiple methods for user authentication. For example, in iPhone 6s, there are:

- Swipe (no security)
- Pattern (medium security)
- Passcode (medium to high)
- Fingerprint (high)

Usability has always been an important issue when implementing security. As human being, users always want an easy solution. The most common authentication method used today is combination of username and password from 'what you know' factor. However, users are keen to choose simple passwords which are easy to guess thus negating the whole point of a secure system. QR Code offers a better solution. User does not have to remember those complex and complicated passwords. User only need to install the mobile application (one time only) and bring his personal smartphone to get authenticated. As mentioned before, user has the option to add more security layer to the smartphone by setting the screen lock security. Since smartphone has become a common device for users and QR Code generation is just one click away, this combination is chosen to be used for the authentication method.

Visible light communication (VLC) has a promising future and opens up new possibilities in location-based authentication. VLC uses LED for illumination and data communication simultaneously. LED is classified as a green technology and more environmental friendly compared to the conventional lighting devices as it has lower power consumption and lower voltage, longer lifetime, smaller size and cooler operation [9]. LED lightbulbs are widely used in many infra structure including homes, offices, street and traffic lights and smartphones [10]. These existing LED lightbulbs can be used as the transmitters which can greatly reduce the cost of the system.

Current smartphones have the capabilities to serve as the VLC receiver. The majority of new generation smartphone have built-in Complementary Metal-Oxide Semiconductor (CMOS) cameras that are capable to capture photos and videos. In [11], a proof-of-concept has been established to demonstrate that a CMOS camera sensor on a smartphone is able to capture data from a VLC transmitter. A similar approach but with an improved data rate was proposed in [12] where the message was encoded using Red, Green and Blue (RGB).

Since the beacon signal from the VLC transmitter is used as the indicator on the location of the user, it is very important that the signal is confined within the protected area. Due to the properties of the light, the signal does not pass many common building materials. However, it may be possible for a leakage of signal through a window or beneath a door. To limit the risk of the exposure, it is advisable that the protected area is covered. The windows should be tinted and installed with curtains. The door should also be covered to avoid the light from going out from the area through the sides of the door. The physical security should also be taken into consideration. LED transmission module which contains the private symmetric key should also be protected from being stolen.

Another promising communication technology that can be implemented in this solution is Li-Fi. Li-Fi, an abbreviation for Light Fidelity is another form of Visible Light Communication technology which delivers high-speed, bidirectional and networked mobile communication. The term Li-Fi was first used by University of Edinburgh Professor Harald Haas during Technology, Entertainment and Design (TED) conference in 2011 [13]. Promising benefits such as greater frequency bandwidth spectrum (10,000 times larger than radio wave) and fast data transmission rate (theoretically speeds up to 224 Gbps) make Li-Fi technology a hot topic in data communication today [14]. Li-Fi technology has yet to be commercialized but it offers a great opportunity for location based authentication system. In the proposed solution, Li-Fi could be used as both data communication medium and also for broadcasting beacon message to verify the location of the user.

4. RELATED WORKS

This section reviews some of the related works that have been proposed over the past few years with regards to location based authentication system. As far as the authors are concern, there is no existing proposal of location based authentication system which combine components such as time-based crypto key and VLC technology to verify location information and smart phone with QR Code as the user-friendly authentication method. So the discussion on the related works will be largely centered around those components.

In [15], the author proposed a system with similar implementation where time-based one-time passwords (OTP) are broadcasted at regular intervals by a transmitter using Bluetooth Low Energy [BLE] technology. When a user wishes to authenticate to the system, the user executes the OTP authentication application on the user's smartphone. The application generates an OTP based on the device and user-specific secret. At the same time the application also scans for the broadcasted time-based OTP from the transmitter. The application then sends both OTPs to the server to be verified. The user will be authenticated if both OTPs are valid. Since the system uses Bluetooth technology to broadcast the OTP, it could not be used to confine the permitted area within a small room. Bluetooth signals can penetrate walls, thus devices located at neighboring rooms could still capture the OTP message. BLE is only supported on limited types of devices. Bluetooth is also usually not activated on devices as users often perceive it as a battery hog. Our proposed system uses similar technique to confirm location information of the users but with different broadcast medium. VLC is used because the coverage area for the beacon messages can be controlled better.

Authors in [16] presented a concept called WifiOTP aims to simplify user interaction for system requiring two-factor authentication. A Wi-Fi access point broadcasts a periodically changing SSID that contains the encrypted OTP together with other data (e.g. system ID etc.). A connector application or a service/daemon running on the client device then scans the broadcasted SSIDs periodically or when initiated by users. The current OTP (decrypted by the client application) is send to the server together with the first authentication method (username and password) to be verified. In the proposed solution, the location information of the user is used as the second authentication factor without requiring user interaction during the authentication process. Wi-Fi signals can also penetrate walls which make it inadequate to restrict the permitted area within a small room. Another limitation of this system is the user may still need to type in the correct combination of username and password. Simple and short passwords are easy to guess and be broken. However, complex and long passwords are difficult to remember. Our solution uses QR Code which offer a convenient and friendly method for users to get authenticated. User do not need to type in complex username/password to get authenticated.

There are some proposed solutions that are working on room-level proximity. In [17], the authors proposed a technique to recognize whether or not users exist in the same room with a size approximately equal to 5 meters square. The technique is based on similarity of received signal strength (RSS) of beacons frames received from ambient multiple access points. Before a connection is established between a client and a server, the client calculates the mean of RSS from beacons frames observed from multiple access points and send the result to the server. The server compares the result with a predetermined threshold to decide whether or not the client is in the same room as the server is. From the experiments, the authors claimed that they have achieved recognition accuracy of more than 95% with the approximated room size. However, the recognition accuracy deteriorates in larger rooms. In [18], the same authors proposed an improved technique that can detect users who are in the same room with high accuracy even though they are 10 m away. In the improved technique, both 2.4 GHz and 5 GHz signals which have different propagation characteristics are used. Both systems require at least two trusted devices in the same room which can be considered a major drawback. Our proposed system is more cost effective as it requires only one VLC transmitter to indicate location information. The transmitter serves two purposes which are to broadcast beacon messages and at the same time provide illumination to the room. Our proposed system also works further to use the location information as an input authentication parameter. As for user-friendly feature, a typical smart phone that displays QR code is used as authentication method. Users do not have to memorize complex password. Users also do not need to purchase new object as the authentication method. The cost of a smart phone nowadays is very affordable and smart phone has become a common gadget for people.

5. CONCLUSION

In this paper, a new location based authentication system is presented. The proposed system allows system administration to enforce a strict security policy which is required for highly secured system such as military, secret service etc. Under the policy, only access from a small confined area such as a small control room is allowed. The proposed system makes use of visible light communication (VLC) technology that broadcasts time-constrained beacon message to be captured by the user's personal smartphone. The message coupled with the crypto response from the personal smartphone are then used to generate a QR Code. Finally, the QR Code is send to the server to be verified. The resulting message from the QR Code is used to confirm two things. First, the logging user is located within the permitted area and second, user has possession of the personal smartphone. The solution is cost effective. With the exception of the circuit for VLC transmitter, the solution does not require infrastructure changes. The use of QR Code within the smartphone offers users a hassle-free but secure method to authenticate to a system. To the best of our knowledge, this is the first model that combines VLC technology, QR Code and crypto engine inside a smartphone to provide a secure location based authentication system.

ACKNOWLEDGEMENT

This research is funded by Universiti Kebangsaan Malaysia (UKM) research project GGPM-2016-011 and is carried out under the Network and Communication Technology Research Lab, Research Centre for Software Technology and Management (SOFTAM), www.ftsm.ukm.my/softam, Faculty of Information Science and Technology.

REFERENCES:

[1] M. S. Kirkpatrick, G. Ghinita, and E. Bertino, “Privacy-preserving enforcement of spatially aware rbac,” IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 5, pp. 627–640, September 2012.

[2] E. Bertino and M. S. Kirkpartrick, “Location-based access control systems for mobile users: Concepts and research directions,” in Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, ser. SPRINGL ’11. New York, NY, USA: ACM, 2011, pp. 49–52. [Online]. Available: http://doi.acm.org/10.1145/2071880.2071890

[3] http://www.ipligence.com, [Retrieved 9 September 2016].

[4] http://www.maxmind.com, [Retrieved 9 September 2016].

[5] http://www.quova.com, [Retrieved 9 September 2016].

[6] http://www.ip2location.com, [Retrieved 9 September 2016].

[7] “Ict: Facts & figures.” [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

[8] T. Bradley, “Would you realize if you lost your smartphone,” PCWorld, May 2011.

[9] K. Sindhubala and B. Vijayalakshmi, “Ecofriendly data transmission in visible light communication,” in Computer, Communication, Control and Information Technology (C3IT), 2015 Third International Conference on, Feb 2015, pp. 1–4.

[10] Y. Wang, N. Chi, Y. Wang, L. Tao, and J. Shi, “Network architecture of a high-speed visible light communication local area network,” IEEE Photonics Technology Letters, vol. 27, no. 2, pp. 197–200, January 2015.

[11] C. Danakis, M. Afgani, G. Povey, I. Underwood, and H. Haas, “Using a cmos camera sensor for visible light communication,” in 2012 IEEE Globecom Workshops, Dec 2012, pp. 1244–1248.

[12] “Casio unveils prototype of visible light communication system using smartphones at ces,” 2012. [Online]. Available: http://arch.casio.com/news/2012/0115_VisibleLightcomm

[13] H. Haas, “Visible light communication,” in Optical Fiber Communications Conference and Exhibition (OFC), 2015, March 2015, pp. 1–72.

[14] D. A. Basnayaka and H. Haas, “Hybrid rf and vlc systems: Improving user data rate performance of vlc systems,” in 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), May 2015, pp. 1–5.

[15] R. van Rijswijk-Deij, “Simple location-based one-time passwords,” Utrecht, Tech. Rep., 2010.

[16] E. Huseynov and J.-M. Seigneur, “Wifiotp: Pervasive two-factor authentication using wi-fi ssid broadcasts,” in ITU Kaleidoscope: Trust in the Information Society (K-2015), 2015, Dec 2015, pp. 1–8.

[17] Y. Agata, J. Hong, and T. Ohtsuki, “Room-level proximity detection using beacon frame from multiple access points,” in 2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), Dec 2015, pp. 941–945.

[18] Y. Agata, J. Hong, and T. Ohtsuki, “Room-level proximity detection based on rss of dual-band wi-fi signals,” in 2016 IEEE International Conference on Communications (ICC), May 2016, pp. 1–6.