Achieving load balancing between privacy protection level and power consumption in location based services

Mohamad Shady Alrahhal[1], Maher Khemekhem[2], Kamal Jambi[3]

[1]King Abdul-Aziz University, Faculty of Computing and Information Technology, Jeddah, Saudi Arabia
[2&3] Full Professor, Abdul-Aziz University, Faculty of Computing and Information Technology, Department of Computer Science, Jeddah, Saudi Arabia
E-mail: [1]shady.rahal1986@gmail.com, [2]maherkhemekhem@yahoo.com, [3]kjambi@kau.edu.sa

Abstract - *Recently, Location Based Services (LBS) have become popular due to the openness of the wireless networks and the development of smartphones. During using the LBS, the LBS users are forced to reveal some private information, such as their accurate locations that can be tracked by malicious parties to attack the privacy. The researchers responded by proposing various user-based approaches to preserve the privacy of the LBS users based on guaranteeing a high k-anonymity level. However, increasing k-anonymity level leads to more power consumption, which in turn drains the battery of the smartphone. Achieving Load balancing between the users' privacy protection level and the power consumption of the smartphones have not been addressed to the best of our knowledge. In this paper, we propose a customized power consumption model specialized for LBS-enabled applications to solve the tradeoff between privacy protection level and power consumption. Six factors are used to build the proposed model, which are backlight, CPU, WiFi, memory, bandwidth, and GPS. The power consumption of each factor is adjusted by the execution time of the privacy protection method. Our proposed power consumption model tested on a various dummy-based privacy protection approaches, and the results showed the best k-anonymity value with respect to the power consumption.*

Key Words*: *Dummy, Factors, Power Consumption, Privacy Protection, Smartphone.

1. INTRODUCTION

Recently, there has been a rapid development in the world of mobile technology and Internet Networking, resulting in a variety of new mobile devices and social networks as well as the development of emerging Internet of Things (IoT) services [1, 2, 3, 4, 5]. Most of these developments rely on location-based services (LBS). IoT devices, smartphones, as well as LBS all have built on Global Positioning System (GPS) with a powerful computation capability. Users can easily get the benefits of LBS applications through downloading them from various sites such as the Apple Store or Google Play Store. With the help of these applications, users can send their queries together with their identities, locations, interests, and other information (e.g., time, query range) to the LBS server. In return, they enjoy the benefits provided by LBS such as searching for the Points of Interests (POI) like the nearest shopping mall, supermarket, restaurant [6], or even ask help in emergency situations [7]. Moreover, integrating LBS applications with wireless communication technologies have enabled the creation of location-based social networking services, such as Foursquare, Twinkle, and GeoLife [8]. This integration bridges the gap between the physical world and the digital online social networking services, opening the door to new challenges.

One of the most important issues, which stands as a big challenge in the LBS research field, is privacy protection. Privacy protection means that the personal information, that may be revealed during using LBS-enabled applications, must be protected. Personal information can be collected from the sensitive data included in the query sent to the LBS server. Figure 1 illustrates the classical scenario of using LBS enabled applications.

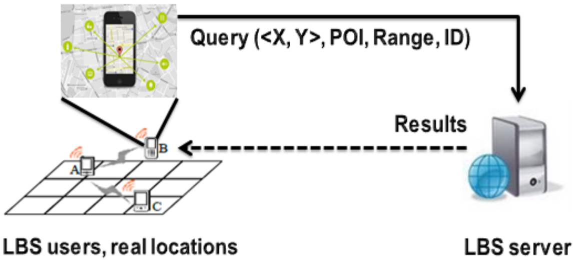

Figure -1: The Classical Scenario of Using LBS-enabled Applications.

As shown in Figure 1, the LBS user sends a query of the form $(\langle x,y\rangle, POI, Range, ID)$. $\langle x,y\rangle$ denotes the coordinates of the real location of the LBS user, POI denotes the queried Point of interests, $Range$ denotes the space of searching, and ID denotes the identity of the LBS user. The sent query can be analyzed and the real location can be tracked by an attacker, resulting in two types of privacy: query privacy and location privacy. These types of privacy must be protected to say that we have a full privacy protection.

The researchers responded by building defenses against the attacker to protect the privacy of the LBS users. In the field of LBS, privacy protection approaches are classified into two main categories: user-based approaches and server-based approaches [9, 10, 11]. Each category has its own techniques, as shown in Figure 2.

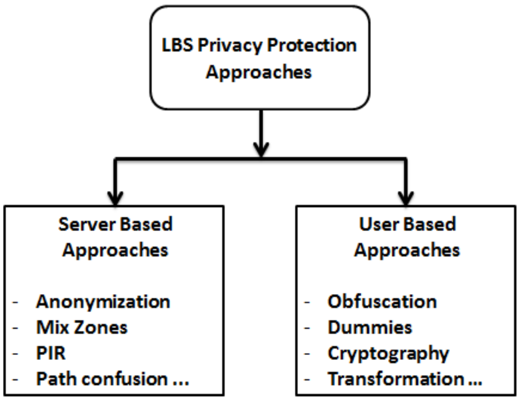

Figure -2: Classification of LBS Privacy Protection Approaches.

In the server-based approaches, the LBS server is considered a Trusted Third Party (TTP), where the protection method is installed there. However, the LBS server can act as a malicious party, which form the main disadvantage of this category. That is because all information stored on the LBS server, about the users, will be accessible. This changed the mind of the researchers to move to the user-based category. In the user-based approaches, the LBS server is considered an attacker and has the ability to analyze the queries and track the real locations of the users. In addition, the LBS user has a full control of the privacy protection method since it is installed on his/her mobile device. However, the main disadvantages of the user-based approaches are that the mobile device of the LBS user suffers from the storage limitation, low computational capabilities, and short lifetime battery.

Motivation. In both categories, the approaches achieve the k-anonymity concept. K-anonymity concept aims at preventing the attacker from determining the query issuer (i.e., the real LBS user) among the others. Here, the level of the prevention mainly depends on the k value, where high k-value is preferred. That is because a higher k value means a higher privacy protection level. This, in turn, requires a long processing time and consumes the power of the mobile device, especially when the LBS user performs any privacy protection approach that belongs to the user-based category. Therefore, there is a tradeoff between the k-anonymity value and the power consumption of the mobile device that must be deal with efficiently.

The contribution of this paper is as follows:

- We define six factors (or components) that are involved in the power consumption of the smartphones. These factors are backlight, CPU, WiFi, memory, bandwidth, and GPS.
- Based on the sixth defined factors, we introduce a novel power consumption model customized for the LBS-enabled applications on the smartphones.
- Based on the proposed power consumption model, we test several user-based privacy protection approaches to estimate the best K-anonymity value that achieves load balancing between the privacy protection level and the power consumption.

The rest of this paper is structured as follows: in section 2, we discuss the related work. Section 3 provides the factors that consume the most power of the smartphones. In section 4, we present our proposed power consumption model. The experimental results are presented in section 5. Finally, we conclude the paper in section 6.

2. RELATED WORK

In this section, we review some works proposed previously in power consumption models and some other works related to the user-based privacy protection in LBS research field.

2.1 Power Consumption Models

There is a wealth of research studies on power models in the existing literature. Some of them specifically target smartphones but depend on external hardware to measure the actual current charge consumed by individual components of the smartphone.

PowerScope was provided in [12] as a tool, which uses hardware instrumentation to measure the power consumption of mobile applications. Some more recent works based on state-based models of the machine to measure the power consumption, such as [13] and [14]. In [13], the authors divided the system into states and associate a fixed power consumption value to each state by modeling the device as a finite-state-machine. The authors of [14] developed the previous, where they employed a seemingly comprehensive set of training and characterization applications in order to construct a model with power usage cost assigned to pre-defined states.

Another statistical power-based model was proposed in [15]. The goal of this model is to achieve a high rate power estimations. The strong feature of this model is that it is adaptive with the machines and can be used for Linux-based smartphones including Nokia and Android. Targeting the better energy management, the authors of [16] tried to model the power consumption based on the darkening parts of the mobile organic light-emitting diode (OLED) display. The key idea of this model is to analyze the power consumption depending on the average pixel color of the screen.

2.2 User-Based Privacy protection Approaches

The authors of work [17] proposed a dummy data array (DDA) algorithm for generating dummy locations to protect the location privacy of LBS users. For a given region, which is divided into a grid of cells, the key idea of the DDA algorithm is to calculate both the vertices and the edges of each cell in the grid. Then, the DDA algorithm randomly selects some of the cells as dummy locations. To select strong dummy locations and achieve k-anonymity, the DDA algorithm selects k cells of equal area. Similarly, [18] uses dummies to protect the location privacy of LBS users, but with a different dummy generation method. The authors proposed two algorithms. The first is called CirDummy, which generates dummies based on a virtual circle that contains the real location of the LBS user. The second is called GridDummy, which generates dummies based on a virtual grid that covers the real location of the LBS user. In [19], a dummy generation method called the Destination Exchange (Dest-Ex) method was proposed. In this method, historical motion trajectories are used to generate the dummies. To ensure that the generated dummies are strong, the Dest-Ex method chooses the historical trajectories that intersect with the current trajectory of the LBS user. Therefore, the attacker is confused when trying to determine the correct LBS user, who has several motion trajectories with different destinations.

For other privacy protection techniques used on the user side, a wide spectrum of these techniques can be explored in [21].

3. FACTORS OF SMARTPHONE POWER CONSUMPTION

In this section, we define the factors that consume the most power of the smartphones.

Form energy perspective, there are four elements that involve in the power consumption of a smartphone: user, environment, software, and hardware. Figure 3 gives a general overview of the energy causes in the smartphones.

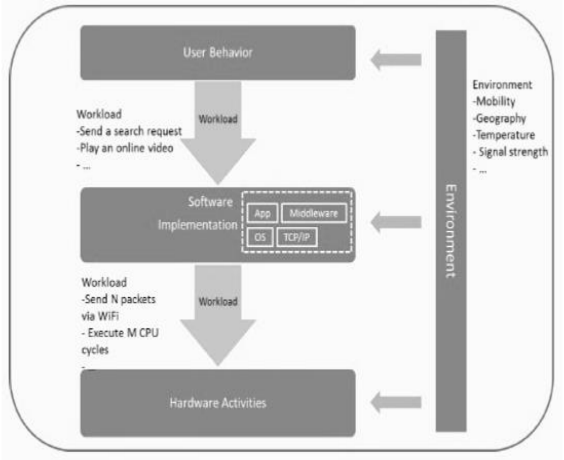

Figure -3: Overview of The Energy Causes.

Despite the fact that each application installed on a smartphone contributes differently to its battery drain during the execution, there are fundamental factors (or components) that consume the most power of the smartphones, as described below.

3.1 Backlight

The backlight is defined as a form of illumination used in liquid crystal displays (LCDs). Smartphones have larger screens compared to the traditional phones. Consequently, they require more LCDs, which in turn consumes more power. In-depth, the bigger the display gets the more LEDs are needed, also the more pixels the display contains for higher resolution the more LEDs are required to brighten up the display. The minimum backlight power is approximately 7.8 mW and the maximum 414 mW [20].

3.2 Bluetooth

Bluetooth is defined as a telecommunications industry specification which describes how smartphones can easily communicate with other devices using a short-range wireless connection. Bluetooth is mainly used for sharing files. During sharing a file, a three main process is performed: Bluetooth on, scanning for devices, and data transfer. The total corresponding power consumption is 36 mW [20].

3.3 CPU

The CPU is the smartphone's component that drains the most power of the battery. The relationship between the CPU and power consumption is that the faster a processor, the more power it consumes.

3.4 WiFi

The smartphones are equipped with a WiFi network interface. When a smartphone connects or tunes a WiFi network, it consumes power. [20] showed that the power consumption in connection is 868 mW.

3.5 Cell Radio

The calls of smartphones are made over Global System for Mobile communication (GSM) cellular service, which costs the battery some power consumption. During the phone call, GSM consumes 800 mW on average [20].

3.6 Memory

Many activities are performed on the content of the memory of the smartphones, which consumed the power. Among the activities, read and write (or store) data processes drain the most of the power.

3.7 Band Width

In smartphones, this term refers to the data transferring between the memory and the other components of the smartphone, which also consumes some power.

3.8 Global Positioning System (GPS)

The power consumed by the GPS mainly occurs when the GPS is enabled. [20] showed that it consumes 166.1 ± 0.04 mW.

4. OUR PROPOSED POWER CONSUMPTION MODEL

In this section, we determine the factors that consume the power when an LBS application runs on a smartphone. Then, based on the determined factors, we present the power consumption model. In addition, we present the strategy of determining the best k value that achieves load balancing between the privacy protection level and the power consumption.

4.1 LBS-enabled Applications and Power Consumption Factors

All LBS-enabled applications use a common location engine (referred to GPS) that runs on the smartphones. When an LBS application is installed on a smartphone and begins to run, the CPU consumes a fraction of power for data processing. The location engine, in turn, uses a database of known access points and their associated locations (latitude and longitude). This database is loaded as a hash table into the smartphone memory at runtime for fast access. Each time the location is computed, the WiFi network card is made to scan for visible access points, and subsequently, the location of these access points is retrieved from the database. This, in turn, means that memory and WiFi consume additional two fractions of power. Because of the continuous updates of the location (during mobility), the new locations are computed by the GPS, which in turn consumed a new fraction of the power. The interaction between the CPU and memory (i.e., both communications and data transferring represented by bandwidth) needs a fraction of power also. Backlight consumes another fraction of power due to a variety of the pixels' brightness. In regarding the Bluetooth and cell radio factors, they are not involved in the power consumption when an LBS application is running on the smartphone. Therefore, the corresponding fractions are ignored.

From the description presented above, six factors are involved in the power consumption in regarding run an LBS application. During time progress, each factor drains a different amount of power. The variety of the amount of power drained by each factor is adjusted by the behavior of the LBS application that is executed on the smartphone. Figure 4 shows the six factors encapsulated with the behavior of LBS application.

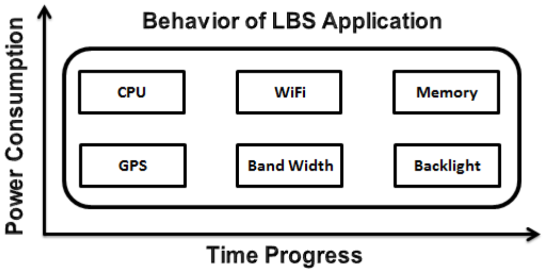

Figure -4: Power Consumption Factors of LBS.

4.2 Customized Power Consumption Model

Mathematically, the fractions of power consumption illustrated in Figure 4 are modeled as separated power consumption units. Let PCU denotes the power consumption unit as a factor or component. Then, each factor has its own PCU, which are: PCU_{cpu}, PCU_{wifi}, PCU_{mem}, PCU_{gps}, PCU_{bw}, and PCU_{bl}.

During time progress, each PCU has different values. This results in a non-leaner curve. Therefore, we need integration formulas to calculate the cost of power consumption of each unit. Let C_{unit} denotes the cost of a given PCU. Then,

$$C_{cpu} = \int PCU_{cpu} \quad (1)$$
$$C_{wifi} = \int PCU_{wifi} \quad (2)$$
$$C_{mem} = \int PCU_{mem} \quad (3)$$
$$C_{gps} = \int PCU_{gps} \quad (4)$$
$$C_{bw} = \int PCU_{bw} \quad (5)$$
$$C_{bl} = \int PCU_{bl} \quad (6)$$

The boundaries of each integration are dominated by the behavior of the LBS application, which in turn limited by the moments of starting and finishing execution time. In details, for a given LBS application $(lbs - app)$, let T_{exe} denotes the execution time of starting moment t_s and finishing moment t_f. Then, the previous formulas are updated to be as follows:

$$C_{cpu} = \int_{t_s}^{t_f} PCU_{cpu}\ d(t) \quad (7)$$
$$C_{wifi} = \int_{t_s}^{t_f} PCU_{wifi}\ d(t) \quad (8)$$
$$C_{mem} = \int_{t_s}^{t_f} PCU_{mem}\ d(t) \quad (9)$$
$$C_{gps} = \int_{t_s}^{t_f} PCU_{gps}\ d(t) \quad (10)$$
$$C_{bw} = \int_{t_s}^{t_f} PCU_{bw}\ d(t) \quad (11)$$
$$C_{bl} = \int_{t_s}^{t_f} PCU_{bl}\ d(t) \quad (12)$$

Consequently, the total power consumption of an LBS application $(T_{pc}^{lbs-app})$ is presented as:

$$T_{pc}^{lbs-app} = C_{cpu} + C_{wifi} + C_{mem} + C_{gps} + C_{bw} + C_{bl} \quad (13)$$

4.3 Strategy of Determining The Best Privacy Protection Level

In general, the privacy protection level is determined by the k-anonymity value. When k value increases, the privacy protection level increases. At the same time, increasing the k value leads to more power consumption since the time of execution of the LBS application increases. In other words, the relationship between the power consumption and the LBS application (supported by a privacy protection technique) is: increasing k value leads to increase the power consumption. To determine the best k value with respect to power consumption, we can find the intersecting point between the corresponding curves of the two aspects.

In steps, let PPL denotes the privacy protection level and PC denotes the power consumption. Then, the first and second steps are to draw the corresponding curves of PPL and PC as functions to k.

$$PPL = f(k) \qquad (14)$$
$$PC = f(k) \qquad (15)$$

Regarding the PPL, it is quantified by using the entropy privacy metric (E) [21]. Therefore, we can get the results by implementing some privacy protection approaches, such as DDA [17], GridDummy [18], CirDummy [18], and Dest-Ex [19]. After obtaining the results (i.e., E values), we can draw the curves that correspond to the formula (14). In regards to the PC, we use the Trepn Profiler benchmark to calculate the power consumption of each factor provided by the formula (13). Trepn Profiler is an Android application that can display the real-time power consumption on a smartphone or tablet [22]. After obtaining the results (i.e., PC values), we can draw the curves that correspond to the formula (15).

As a third step, we can extract the best k value by graphically calculating the intersection point of the two curves.

5. EXPEREMANTAL RESULTS

We implemented the three privacy protection approaches presented in the previous section on a smartphone with specifications collected in Table 1.

Table -1: Specifications of Smartphone.

Component	Description
Processor	1 GHz Qualcomm QSD 8250 Snapdragon ARM
LCD	SLCD capacitive touchscreen %
Wi-Fi	Wi-Fi IEEE 802.11b/g/n
GPS	aGPS
Cellular	STC KSA GSM/UMTS/HSPA
Audio	Built-in microphone and speaker
Battery	Internal Rechargeable Li-ion: 1400 mAh
OS	Android 2.3.3 (Gingerbread)

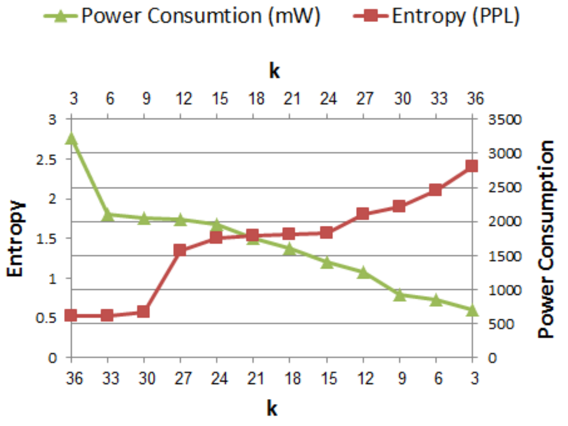

Figure -5: Best k Value for The GridDummy Privacy Protection Method.

Figure 5 shows that the best k value is 18, which meets a power consumption about 1600 mW. The power consumed by applying GridDummy is high a little bit. That is because this privacy protection method depends on calculating the vertices of the grid to select the dummy locations that protect the privacy of the BS user. This tacks a considerable time, which in turn increases the execution time of the GridDummy method. Since the execution time is long, the corresponding power consumption is high.

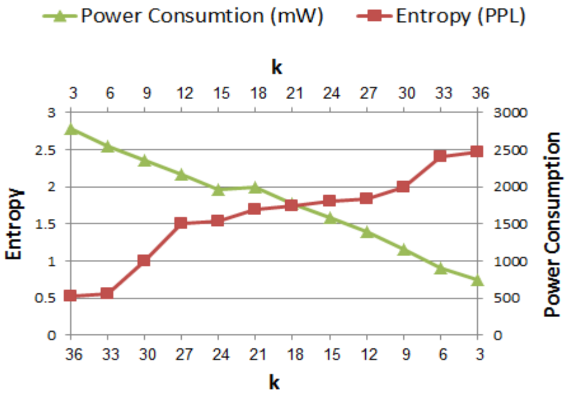

Figure -6: Best k Value for The CirDummy Privacy Protection Method.

As shown in Figure 6, the best k value that achieves load balancing with power consumption is 21. This, in turn, reflects the strength of CirDummy privacy protection method, where the entropy values are higher than the GridDummy. The corresponding power consumption is about 1990 mW, which is higher compared to the GridDummy. That is because of the CirDummy method selects the dummy locations within a specific circle. After defining the circle, the vertices of the grid are calculated. Therefore, the execution time of the CirDummy is longer than the execution time of the GridDummy, which leads to more power consumption.

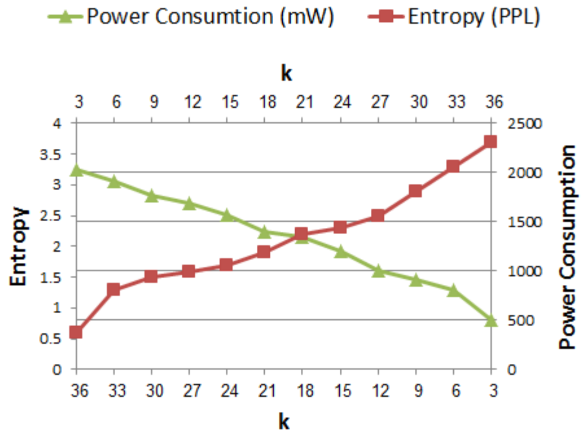

Figure -7: Best k Value for The Dest-Ex Privacy Protection Method.

Similar to CirDummy, Figure 7 shows that the best k value is 21. Compared to the GridDummy and the CirDummy, the corresponding power consumption when using Dest-Ex privacy protection method is 1400. This lower power consumption could be justified by the nature of selecting the dummy locations in the Dest-Ex privacy protection method. Here, the process of selecting dummy locations is performed automatically based on the actual motion trajectory of the LBS user. This leads to lower computations and shorter execution time, which consequently leads to a lower power consumption.

For the DDA privacy protection method, Figure 8 below shows that the best k value is 17 with corresponding power consumption of 2000 mW. Compared to the GridDummy, CirDummy, and Dest-Ex privacy protection methods, the DDA privacy protection method performs the worst at both levels privacy protection and power consumption. That is because the DDA fills the array of dummies by selecting locations in a random way based on the principle that "the dummy locations must be equal in the area". Therefore, the DDA needs to calculate the area of each cell and then select the cells that are equal in area to be the dummy locations. This, in turn, drains a high power consumption.

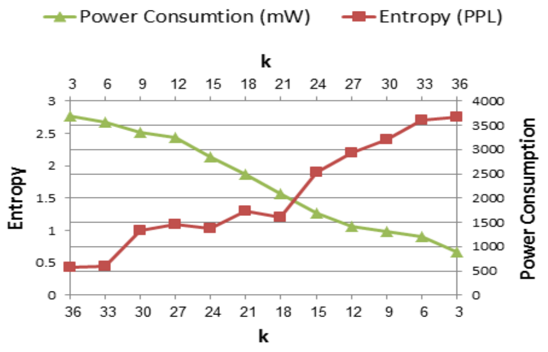

Figure -8: Best k Value for The DDA Privacy Protection Method.

5. CONCLUSION

Power consumption is a vital research field, especially when it comes to talking about smartphones, where the lifetime of the battery is short. In LBS-enabled applications supported by a privacy protection techniques, the power of the smartphone is massively drained according to the execution time of the privacy protection technique. Motivated by this fact, we proposed a power consumption model that achieves load balancing between the power consumption and the privacy protection level. To build the model, we addressed the fundamental factors that consume the most of the smartphone's power. Out of these factors, we selected the factors that are involved in the power consumption in LBS-enabled applications supported by a privacy protection methods. Many dummy-based approaches that are used to protect the location privacy of the LBS users were tested to extract the best k-anonymity value, which leads to the optimal privacy protection level with the corresponding power consumption values. The results showed that there is a variety of the k values according to the mechanism that is used in the dummy-based privacy protection approaches.

In the future work, we intend to generalize the proposed power consumption model to cove other privacy protection methods, such as obfuscation, cryptography-based and coordinates transformation privacy protection techniques.

REFERENCES

[1] Chang, Victor, Verena Kantere, and Muthu Ramanchadran. "Emerging Services for Internet of Things." (2017).

[2] Leminen, Seppo, Mervi Rajahonka, and Mika Westerlund. "Actors in the Emerging Internet of Things Ecosystems." International Journal of E-Services and Mobile Applications (IJESMA) 9.1 (2017): 57-75.

[3] Ghanbari, Amirhossein, et al. "Business development in the Internet of Things: A matter of vertical cooperation." IEEE Communications Magazine 55.2 (2017): 135-141.

[4] Taleb, Tarik, et al. "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Architecture & Orchestration." IEEE Communications Surveys & Tutorials (2017).

[5] He, Wu, Gongjun Yan, and Li Da Xu. "Developing vehicular data cloud services in the IoT environment." IEEE Transactions on Industrial Informatics 10.2 (2014): 1587-1595.

[6] foursquare, online, available: http://foursquare.com/, retrieved Apr 15. 2017.

[7] General Motors, ―Onstar.‖, online, available: http://www.onstar.com/ web/portal/home, Retrieved Apr 15. 2017.

[8] Zheng, Yu, et al. "GeoLife2. 0: a location-based social networking service." Mobile Data Management: Systems, Services and Middleware, 2009. MDM'09. Tenth International Conference on. IEEE, 2009.

[9] Wernke, Marius, et al. "A classification of location privacy attacks and approaches." Personal and Ubiquitous Computing 18.1 (2014): 163-175.

[10] Zhang, Xu, and Hae Young Bae. "Location Positioning and Privacy Preservation Methods in Location-based Service." International Journal of Security & Its Applications 9.4 (2015).

[11] Shin, Kang G., et al. "Privacy protection for users of location-based services."Wireless Communications, IEEE 19.1 (2012): 30-39.

[12] Flinn, Jason, and Mahadev Satyanarayanan. "Powerscope: A tool for profiling the energy usage of mobile applications." Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on. IEEE, 1999.

[13] Pathak, Abhinav, et al. "Fine-grained power modeling for smartphones using system call tracing." Proceedings of the sixth conference on Computer systems. ACM, 2011.

[14] Zhang, Lide, et al. "Accurate online power estimation and automatic battery behavior based power model generation for smartphones." Hardware/Software Codesign and System Synthesis (CODES+ ISSS), 2010 IEEE/ACM/IFIP International Conference on. IEEE, 2010.

[15] Dong, Mian, and Lin Zhong. "Self-constructive high-rate system energy modeling for battery-powered mobile systems." Proceedings of the 9th international conference on Mobile systems, applications, and services. ACM, 2011.

[16] S. Iyer, L. Luo, R. Mayo, and P. Ranganathan, “Energy-adaptive display system designs for future mobile environments,” in Proceedings of the 1st international conference on Mobile systems, applications and services, ser. MobiSys ’03. New York, NY, USA: ACM, 2003, pp. 245– 258.

[17] Alrahhal, Mohamad Shady, et al. "AES-Route Server Model for Location based Services in Road Networks." INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS 8.8 (2017): 361-368.

[18] Lu, Hua, Christian S. Jensen, and Man Lung Yiu. "Pad: privacy-area aware, dummy-based location privacy in mobile services." Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access. ACM, 2008.

[19] Hara, Takahiro, et al. "Dummy-Based User Location Anonymization Under Real-World Constraints." IEEE Access 4 (2016): 673-687.

[20] Naik, Balaji A., and R. K. Chavan. "Optimization in power usage of smartphones." International Journal of Computer Applications 119.18 (2015).

[21] Shin, Kang G., et al. "Privacy protection for users of location-based services." IEEE Wireless Communications 19.1 (2012).

[22] Mostly-Tech, online, available: https://mostly-tech.com/2015/05/28/how-to-measure-the-power-consumption-of-your-mobile-app-using-free-software/

BIOGRAPHIES

First Author Mohamad Shady Alrahhal: PHD student at King Abdulaziz University, KSA, department of computer science, faculty of computing and information technology. Received master degree from Damascus University, Syria, (2013). Received a degree of computer engineering from Albath University, Homs, Syria, (2011). His interest includes security and privacy in social networks, image processing, data mining, machine learning, Big data, and high performance computing.

Second author Maher Khemekhem: Full Professor Department of Computer Sciences, Faculty of Computing and Information Technology King Abdulaziz University. Field of specialization: Distributed systems and OCR. Doctorate degree from Digital Electronics and Computer Science, Digital Electronics and Computer Science, Paris 11, Orsay, France.

Third author Kamal M Jambi: Full Professor Department of Computer Sciences, Faculty of Computing and Information Technology King Abdulaziz University. Received the Ph.D degree from Illio is Institute of Technology, IL, U.S.A, in 1991. He is a full professor with Computer Science dept, Faculty of Computing and Information technology, King Abdullaziz University, Saudi Arabia. His research interests include OCR, NLP, Image Processing, software engineering, big data, distributed systems.