Location Privacy Assured Internet of Things

Ismail Butun and Mikael Gidlund
Department of Information Systems and Technology, Mid Sweden University, 851 70 Sundsvall, Sweden

Keywords: Security, Mix-Zone, Location Obfuscation, IoT, Preserving, Context-awareness, Vulnerabilities, Trust, End-device.

Abstract: Internet of Things (IoT) is in the booming age of its growth, therefore a vast amount of applications, projects, hardware/software solutions, and customized concepts are being developed. The proliferation of IoT will enable location-based services to be available everywhere for everyone, and this will raise a large number of privacy issues related to the collection, usage, retention, and disclosure of the user's location information. In order to provide a solution to this unique problem of IoT, this paper proposes Location Privacy Assured Internet of Things (LPA-IoT) scheme, which uses the concepts of Mix-Zone, location-obfuscation along with context-awareness. To the authors' best knowledge, the proposed LPA-IoT scheme is the first location-based privacy-preserving scheme for IoT that provides flexible privacy levels associated with the present context of the user.

1 INTRODUCTION

The Internet of Things (IoT)[1] is revolutionizing the IT sector. According to predictions, by the end of 2020, 20 billion IoT devices are expected to exist and seamlessly connect each other on the global Internet (Kocakulak and Butun, 2017).

A mobile ecosystem is characterized by devices that usually contain very sensitive personal (and business) data including contacts, communication patterns, and the whereabouts of the user. Hence, one of the major privacy impacts of cyber-security solutions for this ecosystem is the potentially very high sensitivity of attribute disclosure. Similarly, these devices contain information that can easily re-identify their users depending on some preexisting pattern of events such as calendar events, etc.

A somehow similar consideration holds for the IoT ecosystem considering that, for example, home automation systems may continuously detect home activities; health-care related IoT systems may reveal medical conditions, and IoT installations in smart environments may include cameras or other systems that can directly or indirectly identify users performing activities in specific places revealing also their location information at given times. In order to assess the privacy of the users in IoT, algorithms need to be designed. However, following unique properties of the IoT make it challenging to design and difficult to devise algorithms accordingly. Therefore, they create problems to be solved, especially the ones related to privacy (Vasilomanolakis et al., 2015):

- Uncontrolled environment: Users (and in some cases devices) are mobile, IoT devices are physically accessible (especially for adversaries) in public places and finally, there is no trusted authority defined for IoT devices to resume safe operation.
- Heterogeneity: IoT consists of various types of things (devices), services and users.
- Scalability: IoT introduces a highly scalable and flexible network architecture, which may be trouble for the algorithms that are considering stable network conditions.
- Constrained Resources: Some of the IoT things (things and devices are used interchangeably throughout the manuscript) are very tiny and have limited battery power (just as in the case of sensors of WSNs). In order to resume a long lifetime, these devices should be running light-weight algorithms, crafted in accordance with the sleep-wakeup cycles of the devices. These tiny devices have also limited communication (small

[1]This work was supported partially by grants: 20201010 (SMART Project) of the European Regional Fund (ERUF), and 20150367 (TIMELINESS Project) of the Swedish Knowledge Foundation (KKS).

Butun, I. and Gidlund, M.
Location Privacy Assured Internet of Things.
DOI: 10.5220/0007587906230630
In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)*, pages 623-630
ISBN: 978-989-758-359-9

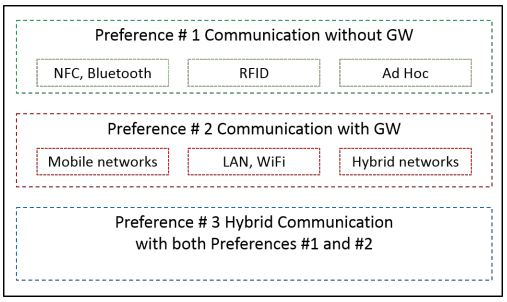

Figure 1: Communications methods in IoT.

area wireless coverage, low data rate, etc.) and computation (small size of RAM, low processing speed, etc.) resources. This limited energy, communication, and computation resources would inevitably dictate design criterion of IoT privacy algorithms/methods/techniques/etc.

Interactions between the things of IoT are achieved via a communication network. Hence, IoT consists of heterogeneous participants; communication in between those devices is a non-trivial task, as it requires multiple protocols to be involved as shown in Fig. 1 (Elkhodr et al., 2013). This heterogeneous nature and distributed architecture of IoT gives rise to numerous security and privacy concerns as summarized as follows (Daubert et al., 2015):

- **Identity Privacy (Visibility).** Who is the data generator? Disclosure of the user identities throughout their IoT interactions should be obstructed.
- **Location Privacy (Where).** Where is the data taken from? The physical location of the IoT users should be preserved so that they will not be tracked.
- **Footprint Privacy (Knowledge).** Can information be extracted from the data being transferred in all layers? Acquisition of large amounts of micro-data should not reveal private information about the users.
- **Query Privacy (Interests).** What was the content of the query? Profiling of the users should be obstructed.
- **Ownership Privacy (Who).** Who is the owner of the data? Data stored in databases or transferred to third parties should not reveal information about who was the owner of the data (which can be used for commercial advertising or business purposes, e.g. quote for the next health insurance agreement).

Over decades, location privacy was a big concern for the users in mobile cellular systems as well as the Internet. As mentioned in (Beresford and Stajano, 2004), Internet Engineering Task Force even formed a special group working only on this issue (Geographic Location/Privacy Working Group). As IoT becoming the next phenomenon in technology just like as Internet, location privacy of the nodes and users will be a primary concern in some specific scenarios, especially the ones related to the critical infrastructures (e.g. location of a valve in a pipeline or location of a critical actuator in a nuclear power plant) and military operations (e.g. position of the friendly forces).

The proliferation of IoT will enable location-based services (LBS) to be available everywhere for everyone, and this will raise a large number of privacy issues related to the collection, usage, retention, and disclosure of the user's location information (Minch, 2015). Therefore, in order IoT to have profound business and societal impacts in our rapidly changing world, location-aware privacy enhancing technologies should be added immediately. This paper aims at providing that.

In order to provide a solution to this unique problem of IoT, this paper proposes Location Privacy Assured Internet of Things (LPA-IoT) scheme, which uses the concepts of Mix-Zone along with location-obfuscation and context-awareness. Mix-Zone provides a masked ID (called pseudonym) for each user whenever users enter a predetermined location zone. No one other than the server knows which pseudonym belongs to which user in the zone. Therefore, from outsider's point of view, the imprecise location of the individual is known (i.e. inside the Mix-Zone) but the precise location is hidden. Similarly, in location-obfuscation, instead of pseudonyms, the precision level of the user's location (that is mostly generated by GPS receiver) is altered (degraded) by an algorithm and then fed to the outsiders. Both of these methods have benefits as well as difficulties. For example, Mix-Zone needs some certain number of users to be in the zone to efficiently mask them. On the other hand, location-obfuscation suffers from communications and processing costs related to the generation of extra levels of (depending on the precision) location information, and also from the handling of that information by the server.

In the proposed LPA-IoT scheme, there is a predetermined threshold level at which the location hiding algorithm changes phase from Mix-Zone algorithm to location-obfuscation algorithm. So that, all the time, location privacy of the users are assured. To the authors' best knowledge, the proposed LPA-IoT scheme is the first location-based privacy-preserving scheme for IoT that provides flexible privacy levels associated with the present context of the user. Besides, the proposed scheme works in a dynamic fashion to provide

best cost efficiency.

The structure of this article is as follows: Section 2 contains a literature review regarding location privacy in IoT. Section 3 overviews location privacy and presents flaws of the existing proposals in the literature. Section 4, where proposed LPA-IoT scheme is presented and discussed follows this. Finally, the article ends with Section 5, which is comprised of conclusions and future work.

2 RELATED WORK

There are solutions in the literature related to providing specific or generic privacy for IoT (data-footprint privacy (Rajagopalan et al., 2011), user configurable privacy enforcement (Henze et al., 2014), relationship of the user privacy and trust (Butun, 2017)), but these works do not establish location-privacy for IoT. Here, authors will present most of the important work related to location-privacy in the literature (some are proposed for IoT, the rest are proposed for mobile and vehicular networks) categorized as follows:

2.1 Context-awareness

The relation in between privacy and context-awareness for IoT is discussed in (Medaglia and Serbanati, 2010). It is concluded that the users may resume two basic operational modes, which are public and private. Based on the context information (Where are we? What we are doing?), privacy can be tuned in: Public operation mode is selected when objects (things) advertise their presence and provide their services to all nearby devices. However, in private operation mode, previously stated functionalities are provided to only very well known (trust wise) neighbors only.

2.2 Location Masking/Cloaking/Obfuscation

Location obfuscation has also known as masking or cloaking, is a method used for protecting location-privacy of the users by generalizing (substituting or altering) the location information. Authors of (Elkhodr et al., 2013) used this method, along with context-awareness to provide location-privacy to general objects (users) of IoT by using data obfuscation techniques.

In (Elkhodr et al., 2013), authors showed how data obfuscation technique could be used to hide precise location information from the unintended parties. In their methodology, they provide three different types of location information and provide this information to the specific type of users/objects. As a result, in the database of each user device; three location data are generated, namely: high-precision, medium-precision, and low-precision. When a highly trusted object or user demands location, high-precise location is provided. Low-precise location is provided to untrusted third party objects/applications/users.

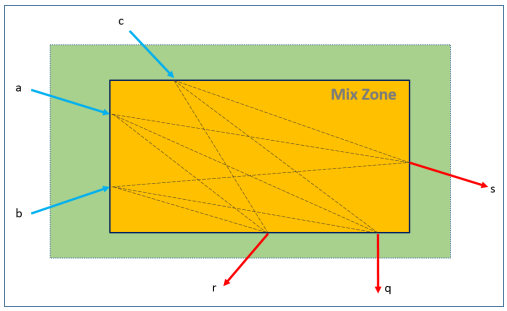

Figure 2: Example movement of three people through a simple Mix-Zone.

2.3 Pseudonymization/Mix-Zone

In (Beresford and Stajano, 2004), authors proposed the Mix-Zone concept for pervasive computing, in which location of the users is masked by the "Mix-Zone". Mix-Zone provides a solution for user privacy in location-based services. It prevents tracking of long-term user movements but still allows the short-term location data to be used by location-aware applications.

After a user enters a Mix-Zone, the specific location of the user right in the Mix-Zone is hidden from the location-aware applications. This way, users inside a Mix-Zone will not be traceable and thereby will have location privacy in that specific zone. These zones may be assigned to a hospital, military facility, etc., in which users do not want to be tracked.

As shown in Fig. 2, for the users a, b and c, the location information is hidden in the Mix-Zone so that they are untraceable. For example, the egress point of user a may be either s, r or q.

2.4 Game Theoretical Approach

In (Freudiger et al., 2009) and (Humbert et al., 2010), authors assume that the Mix-Zone concept of (Beresford and Stajano, 2004) to be used by their system (mobile networks) and they model the willingness (cooperation) of their system users to participate Mix-Zone as a "Game", where each player aims at maximizing its location privacy at a minimum cost.

2.5 Other Approaches

In (Hu et al., 2011) authors proposed identity-based personal location system with protected privacy for IoT. Their proposed architecture includes a client-server relation, which requires a server available all the time and a communication back-haul to support all the transactions. Any location request goes through the server with a classical authentication service: Users with the required credentials are allowed to acquire the personal location information of the subject.

In (Skarmeta et al., 2014), authors proposed capability-based distributed access-control scheme for CoAP (Constrained Application Protocol is a software protocol intended to be used in very simple electronics devices, allowing them to communicate interactively over the Internet) messaging of IoT. This is a distributed approach, in which smart things themselves are capable of making well-defined and context-aware access control decisions. Authors achieved this by designing a lightweight token used for access to CoAP Resources, and an optimized implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) inside the smart things (nodes).

3 DISCUSSIONS REGARDING PREVIOUS WORK

As mentioned in Section 2, the solutions of (Rajagopalan et al., 2011) and (Henze et al., 2014) do not provide privacy for the location information and therefore not promising for assuring location-privacy.

There are solutions in the literature to ensure location privacy for mobile (cellular) networks. As mentioned in (Elkhodr et al., 2012), current privacy issues in mobile platforms are more likely to be inherited if not magnified in the IoT. However, none of the solutions to provide location-privacy to mobile platforms (cellular networks) are tailored to the specific needs and architecture of the IoT yet.

3.1 Context-awareness

The proposed context-aware privacy solution for IoT of (Medaglia and Serbanati, 2010) is a good idea and adopted by this paper. However, authors of the proposal do not provide any algorithms, methods or functions to be used for context-awareness. Therefore, this is left for us as a challenge to tackle.

3.2 Location Masking/Cloaking/Obfuscation

The Dynamic Disclosure Control Method (DDCM) of (Elkhodr et al., 2013) provides six levels of obfuscation levels (from dummy location information towards exact location information) in which different location outputs are generated from the same location information. For example, these five levels of obfuscation can be stated for an address information as follows: Level-0 Exact, Level-1 Street, Level-2 Suburb, Level-3 State, Level-4 County, and Level-5 Dummy (random). The proposed method is valid only for GPS enabled mobile devices. Authors did not discuss the applicability of this method to other IoT devices (with or without GPS). Besides, authors also did not provide any cost analysis, which the proposed DDCM would bring to the IoT systems.

3.3 Pseudonymization/Mix-Zone

As discussed in the literature (Freudiger et al., 2007; Freudiger et al., 2009; Humbert et al., 2010), Mix-Zone model of (Beresford and Stajano, 2004) is not sufficient alone to provide location-privacy. The egress and ingress points of the users can be recorded along with timing information to trace back each user and precisely predict each user's final location after Mix-Zone and a highly correct estimate of the route inside Mix-Zone. Besides, Mix-Zone concept is based upon the collaboration of the users: Users in the Mix-Zone collectively change their pseudonyms to create confusion for the outside observers (attackers). If some of the members selfishly avoid collaborating in the exchange process of pseudonyms, this would decrease the level of confidence in the system (location-privacy).

3.4 Game Theoretical Approach

Although authors of (Alpcan and Başar, 2010) described the zero-sum Nash Equilibrium game in between "attacker" and the "defender"; (Freudiger et al., 2009) and (Humbert et al., 2010) rather to play the game in between "cooperative" and "non-cooperative" users of a location-privacy assured mobile networks. Therefore, application of game theory to location-privacy assured mobile networks (especially the IoT networks) from the perspective of "defender" - "attacker" game remains as a future work to be done.

3.5 Other Approaches

As mentioned in (Notra et al., 2014), other prior work either wrongly addresses the problem (Hu et al., 2011) (classical client-server type authentication is not convenient for highly dynamic and scalable IoT architecture) or propose high-level security architectures (Skarmeta et al., 2014) involving changes to the way IoT devices are currently designed and communicating. With hundreds of IoT device manufacturers, it is almost impossible to come up with a device embedded security solution that caters to all the security and privacy threats for a variety of IoT devices with varying capabilities. Also due to the miniature size of many IoT devices with limited computing capabilities and power resources make it impossible to apply extensive computing-rich security algorithms. Authors also believe that device embedded solutions require all manufacturers to be on board which is a hard task.

Among all previous work in the literature, (Elkhodr et al., 2013) provides a promising solution for assuring location privacy for IoT applications. Although the methodology of the presented work sounds logical, here the problems it represents: It is proposed for generic GPS bearing IoT networks and needs to be tailored for the other kind of IoT networks (with the location sensing devices other than the GPS). Once a precise-data is generated, it is there for hackers and/or high ability users (hired by advertisers, commercial companies, etc.) to capture it. Algorithms and/or methods need to be developed to assure location-privacy, by securing the original precisely generated location data.

3.6 The Distinctive Properties of IoT from "Mobile Networks" and "Vehicular Networks"

Most of the techniques in the literature for assuring location privacy are either devised for "mobile networks" or "vehicular networks". The distinctive properties of IoT from those mentioned networks are as follows:

- Some of the "things" might be stationary, such as sensing devices in the buildings; whereas the other "things" might be mobile, such as devices attached to the users. Hence constituting a heterogeneous structure in terms of mobility.
- Mobility in the IoT is not rapid as in the vehicular networks, hence the mobility mostly related to pedestrians and their surrounding devices.
- The network in IoT needs to be scalable as the number of users and the things might change substantially.
- GPS technology is always available in vehicular networks whereas it might not be available in all nodes of the IoT.
- Some of the "things" in IoT are super-tiny devices, which are intended to save battery life to serve a longer lifetime; hence, the algorithms need to be devised by keeping "energy conservation" in mind. This is not necessary for vehicular networks hence the vehicles have enough battery and power supply all the time.
- In some cases, things of IoT might not be able to connect to the Internet directly but via their neighbors. This brings in the Ad-Hoc Networking concept to the design criterion. Whereas, the vehicular networks are highly connected to Internet or Intranet via Road-Side-Units and/or 2G/3G/4G/5G cellular technology.

4 PROPOSED LOCATION PRIVACY ASSURED INTERNET OF THINGS (LPA-IoT) SCHEME

Context-awareness describes devices that can sense and be aware of their environment to judge their next movement or behavior accordingly. However, location awareness is an also emerging field in mobile applications and portable devices which leads to the introduction of location-based services (LBS) and location-based applications. Location information becomes highly sensitive when it is combined with other contextual information such as the user's identity (Elkhodr et al., 2013).

Location-privacy can be defined as the privacy related to the individuals' location-specific information including their living patterns. As mentioned in (Minch, 2004), usage of location-aware services will arise following location-privacy related implications: collection, retention, use, and disclosure of location information. Extreme consumer profiling can be done by the commercial companies related to shopping and travel patterns of the consumers. Patients visiting health services may be correlated to their health condition which may be very valuable information for health-insurance companies. Moreover, personal safety may be compromised if the location information of individuals is breached.

In an IoT network, location of the users can be determined via one of the methods with the specific ranges provided as follows: GPS (precise, 10 cm - 10

m range), RFID (near-proximity 1 m - 10 m range), WiFi (mid-proximity 10 m - 100 m range), GSM triangulation (far-proximity 100 m - 1,000 m range). Hence the IoT consists of heterogeneous devices, the precise location information as in mobile and cellular networks will not be available all the time.

Mobile Target Tracking (MTT), proposed by Hoh and Gruteser (Hoh and Gruteser, 2005), was able to reconstruct the tracks of mobile devices in a network, indicating that spatial and temporal correlation between successive locations of mobile devices should be carefully eliminated to prevent attackers from compromising the user's location privacy.

The location privacy algorithms provided in the literature (summarized in Section 2) are proposed for either mobile networks or vehicular networks. Hence IoT have distinctive properties and features compared to those mentioned networks (please see Section 3.6), these algorithms cannot be adopted directly. They need to be revised, re-modeled, re-constructed, re-structured in order to fulfill the special requirements of IoT and the users of the IoT.

The design (revising, re-modeling re-constructing, re-structuring) phase of the location privacy algorithm(s) should be followed by a thorough evaluation phase. This evaluation phase should include all the quantification metrics (such as uncertainty, entropy, confusion time, etc.) in order to provide verifiable comparison results.

As mentioned above, location privacy is preventing other parties from a node's past and current location. Hence assuring the location privacy of the IoT nodes is indispensable, the aim of this paper is to provide location privacy with a minimum cost to the IoT nodes.

As discussed in (Medaglia and Serbanati, 2010), location-based services may be provided in two basic operation modes:

1. **Public Mode:** This operation mode would require none or minimal user privacy for location-based services.
2. **Private Mode:** This operation mode would require maximum user privacy for location-based services. This can be achieved by using algorithms to ensure user location privacy, such as the Mix-Zones proposed in (Beresford and Stajano, 2004).

In order to apply this kind of (2-modes of operation: "Public" and "Private") approach, the IoT system needs to be "context-aware", so that it can switch operation mode according to the location the user is visiting.

Our proposed Location-Privacy Assured IoT (LPA-IoT) scheme architecture is shown as in Fig. 3. It consists of mainly three blocks:

- **Context-Aware Engine:** As discussed above, the first block of the proposed LPA-IoT system consists of a context-aware engine, which discovers the current context by comparing the precise location information with the detailed context database (DCDB). DCDB is constituted by the system managers, depending on the applications as well as the user needs. DCDB will be preloaded on all IoT devices of the LPA-IoT system and will be updatable by push-based patches if needed. Patch management aspects of the DCDB is outside the scope of this text. Interested readers on patch management systems may refer to (Al et al., 2012). Our proposed context-aware engine will be similar to the one in (Elkhodr et al., 2013), and accordingly, any context will be analyzed using the following four contextual parameters: Network, Location, Period and Request Owner.
- **Decision Engine:** After the context is specified by the context-aware engine, the result is fed to the decision engine among with the preselected user privacy preferences, in order to conclude the current Privacy Level ("Private" or "Public") to be used for location services. Here, the current context is evaluated with the privacy selection of the user and quantified to be processed by the next block.
- **Location-Privacy Engine:** If the result of the previous engine is "Private", then this block will work, otherwise will not. In order to provide location-privacy, this block uses Mix-Zone concept of (Beresford and Stajano, 2004) and location-obfuscation method of (Elkhodr et al., 2013), both of which are mentioned earlier in this text. According to our proposed LPA-IoT scheme, the location-privacy assuring configuration should be dynamic. According to our proposed model, there is a certain threshold level of the cost that is associated with the number of users in the Mix-Zone, which determines either usage of Mix-Zone approach or not. If not, then the users in the Mix-Zone will have to use location-obfuscation method to attain their location-privacy. The mentioned threshold-level will be determined according to analytical results. Total cost models of both Mix-Zone and location-obfuscation will be determined. These models will include costs related to packet transmissions between server and clients, communications and processing. This will provide us metrics of total cost vs. the total number of users participating. Then, in the same manner, privacy-risk models of both Mix-Zone and location-obfuscation will be determined. This

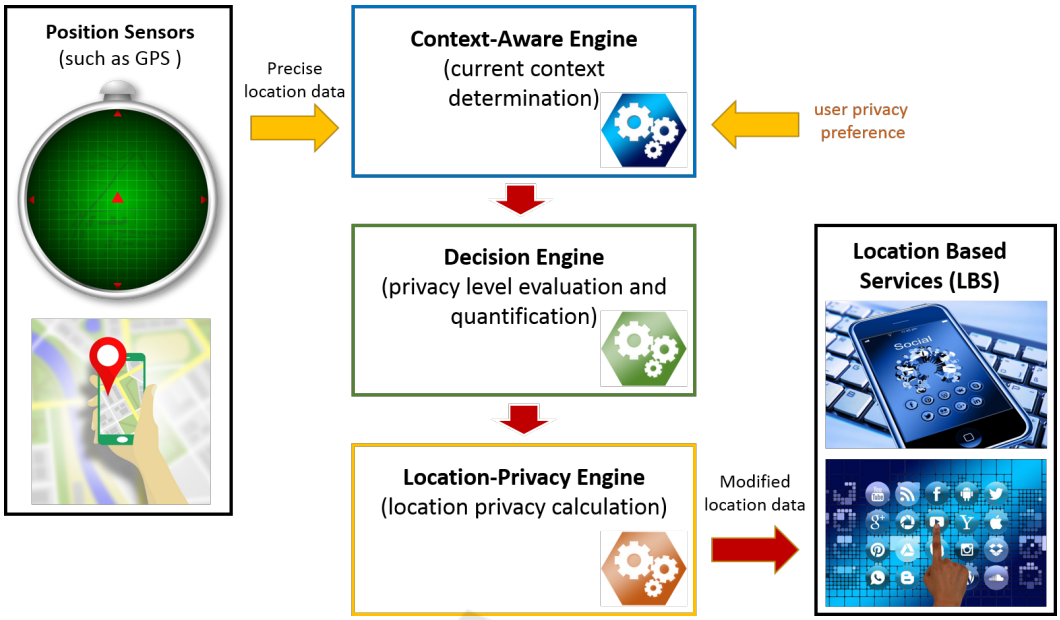

Figure 3: Proposed system architecture for Location-Privacy Assured IoT (LPA-IoT) Scheme.

will provide us metrics of total privacy-risk vs. the total number of users participating. Then by using both obtained metrics, an optimization process will be done to deduce the optimum number of users (N - the threshold-level) where the location-privacy engine will be triggered to switch the main algorithm for the location privacy (i.e. either Mix-Zone approach or location-obfuscation approach). Finally, the decision will be made accordingly on which approach to be used.

The resulting modified-location data from the Location-Privacy Engine block is fed to the information demanding LBS. Here, by modification what authors meant is, depending on the algorithm used in the Location-Privacy Engine block, either the precision of the location (position) in meters (hundreds of meters, etc.) will be changed or the pseudonyms of each location-bearing user will be changed. As a result, the proposed LPA-IoT system assures location-privacy of its users according to their user preference, current context and the total number of users, by using Context-Awareness, Location-Obfuscation and Mix-Zone concepts all together in an ordered and layered fashion.

5 CONCLUSIONS AND FUTURE WORK

With the proliferation of IoT devices, the location privacy of the users will be one of the main concerns related to security. Therefore, in this article, the authors aim at providing a unique solution to address this specific problem.

Several proposals in the literature are reviewed that may be relevant to location-based privacy. Most of the proposals for IoT are aimed at providing different security services rather than location privacy, and a few provided specific solutions for networks other than IoT (e.g. vehicular networks, mobile networks, etc.). Hence, an LBS-based privacy-preserving scheme (LPA-IoT) has been proposed in this paper. To the authors' best knowledge, the proposed LPA-IoT scheme is the first location-based privacy-preserving scheme for IoT that provides flexible privacy levels associated with the present context of the user. The proposed LPA-IoT scheme uses Mix-Zone algorithm for hiding the location information in first place. However, when the total number of users in the zone decreases lower than a certain minimum threshold level, the location privacy cannot be assured. At that point, the proposed LPA-IoT scheme uses the location-obfuscation algorithm. Although this algorithm is most costly compared to Mix-Zone, location privacy is assured by any means, which might be very important in some scenarios.

In the future work, an optimization work (in terms of performance, cost, and privacy) will be done in between Location-Obfuscation and Mix-Zone methods. A threshold level (the total number of users) will be determined according to this optimization result. Besides, evaluation of the performance analysis of the proposed scheme has been also left as a future work.

REFERENCES

Al, F., Dalloro, L., Ludwig, H., Claus, J., Fröhlich, R., and Butun, I. (2012). Networking elements as a patch distribution platform for distributed automation and control domains. Patent App. PCT/US2012/043,084.

Alpcan, T. and Başar, T. (2010). *Network security: A decision and game-theoretic approach*. Cambridge University Press.

Beresford, A. R. and Stajano, F. (2004). Mix zones: User privacy in location-aware services. In *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, pages 127–131. IEEE.

Butun, I. (2017). Privacy and trust relations in internet of things from the user point of view. In *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*, pages 1–5. IEEE.

Daubert, J., Wiesmaier, A., and Kikiras, P. (2015). A view on privacy & trust in iot. In *Communication Workshop (ICCW), 2015 IEEE International Conference on*, pages 2665–2670. IEEE.

Elkhodr, M., Shahrestani, S., and Cheung, H. (2012). A review of mobile location privacy in the internet of things. In *ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2012 10th International Conference on*, pages 266–272. IEEE.

Elkhodr, M., Shahrestani, S., and Cheung, H. (2013). A contextual-adaptive location disclosure agent for general devices in the internet of things. In *Local Computer Networks Workshops (LCN Workshops)*, pages 848–855. IEEE.

Freudiger, J., Manshaei, M. H., Hubaux, J.-P., and Parkes, D. C. (2009). On non-cooperative location privacy: a game-theoretic analysis. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 324–337. ACM.

Freudiger, J., Raya, M., Félegyházi, M., Papadimitratos, P., and Hubaux, J.-P. (2007). Mix-zones for location privacy in vehicular networks. In *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, number LCA-CONF-2007-016.

Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., and Wehrle, K. (2014). User-driven privacy enforcement for cloud-based services in the internet of things. In *Future Internet of Things and Cloud (FiCloud), 2014 International Conf. on*, pages 191–196. IEEE.

Hoh, B. and Gruteser, M. (2005). Protecting location privacy through path confusion. In *Security and Privacy for Emerging Areas in Communications Networks. SecureComm 2005.*, pages 194–205. IEEE.

Hu, C., Zhang, J., and Wen, Q. (2011). An identity-based personal location system with protected privacy in iot. In *Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on*, pages 192–195. IEEE.

Humbert, M., Manshaei, M. H., Freudiger, J., and Hubaux, J.-P. (2010). Tracking games in mobile networks. In *International Conference on Decision and Game Theory for Security*, pages 38–57. Springer.

Kocakulak, M. and Butun, I. (2017). An overview of wireless sensor networks towards internet of things. In *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*, pages 1–6. IEEE.

Medaglia, C. M. and Serbanati, A. (2010). An overview of privacy and security issues in the internet of things. In *The Internet of Things*, pages 389–395. Springer.

Minch, R. P. (2004). Privacy issues in location-aware mobile devices. In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conf. on*, pages 10–pp. IEEE.

Minch, R. P. (2015). Location privacy in the era of the internet of things and big data analytics. In *System Sciences (HICSS), 2015 48th Hawaii International Conf. on*, pages 1521–1530. IEEE.

Notra, S., Siddiqi, M., Gharakheili, H. H., Sivaraman, V., and Boreli, R. (2014). An experimental study of security and privacy risks with emerging household appliances. In *Communications and Network Security (CNS), Conf. on*, pages 79–84. IEEE.

Rajagopalan, S. R., Sankar, L., Mohajer, S., and Poor, H. V. (2011). Smart meter privacy: A utility-privacy framework. In *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, pages 190–195. IEEE.

Skarmeta, A. F., Hernandez-Ramos, J. L., and Moreno, M. V. (2014). A decentralized approach for security and privacy challenges in the internet of things. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, pages 67–72. IEEE.

Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., and Kikiras, P. (2015). On the security and privacy of internet of things architectures and systems. In *Secure Internet of Things (SIoT), 2015 International Workshop on*, pages 49–57. IEEE.