# Internet of Mobile Things: Mobility-Driven Challenges, Designs and Implementations

Klara Nahrstedt, Hongyang Li, Phuong Nguyen, Siting Chang
University of Illinois Urbana-Champaign
{klara, hli52, pvnguye2, schang13}@illinois.edu

Long Vu
IBM T. J. Watson Research Center
lhvu@us.ibm.com

***Abstract*—Smart environments such as smart grid, smart transportation, smart buildings are upon us because of major advances in sensor, communication, cloud and other cyber-physical system technologies. The collective name for interconnected sensors, placed on "things" within fixed cyber-physical infrastructures, is Internet of Things (IoT). IoT enables cities and rural areas to become smarter and to offer new digital services and functions to diverse groups of users. However, IoT often represents interconnection of static things, which are built-in into the physical infrastructures of users' homes, offices, roads and other physical and critical infrastructures. In this paper, we analyze things that are mobile, and explore the space of Internet of Mobile Things (IoMT). Mobility of digital devices such as phones and vehicles has been with us for some time, but as the number of sensors in mobile devices increases, the density of mobile devices increases, and users' reliance on mobile devices increases, mobile things become very much an integral fabric of our smart environment. In this paper, our goal is to discuss challenges, selective designs and implementations of IoMT. We show the impact of mobility and the care we collectively have to take when designing the next generation of smart environments with mobile things in them.**

## I. Introduction

Smart environments such as smart buildings, smart health, smart grid, and smart transportation are upon us because of the advances in sensor technologies, their communication, and their interconnectivity to advanced cyber-physical infrastructures. The interconnected sensors, placed within fixed cyber-physical infrastructures, are collectively named *Internet of Things (IoT)*. IoT represents interconnected static things such as smart meters in smart grid, smart sensors in advanced water systems, RFID and motion sensors in smart buildings, or traffic cameras at road intersections. But in addition to static IoT, mobility of things is coming forward as mobile phones and vehicles are equipped with more and more advanced sensors. The mobile devices with their sensors are then able to communicate with each other, with surrounding cyber-physical infrastructures, and represent the *Internet of Mobile Things (IoMT)*.

The difference between IoT and IoMT is that when considering mobility of things, major changes occur in terms of (a) *context*, e.g., where the mobile device is located, in what hands it is now, (b) *Internet access and connectivity*, e.g., if the mobile device is connected at all, and when connected to what wireless or wired network, at what bandwidth level, and with what security, (c) *energy availability*, e.g., where can the mobile device charge again, how much energy does the mobile app need, (d) *security and privacy*, e.g., what kind of security infrastructure the mobile device encounters when moving among different locations, and what private information do service providers have about user using a mobile device. Hence, when considering IoMT, *mobility* becomes a first class object and one has to look at the IoMT separately from IoT. It is important to note that mobility of devices such as mobile phones and vehicles has been investigated for many years [1]–[5], especially the design of individual devices and their dealings with mobility and usage by users in mobile environments. But what changes now is the increased number of sensors per mobile device, the increased density of mobile devices in users' environments, and most importantly, the increased interconnectivity and the increased reliance of users on mobile devices, making mobile devices and their interconnectivity an integral part of users' daily routines and smart environments.

The goal of this paper is to discuss the IoMT *challenges*, and systems and protocols *design* and *implementation*, where mobility impact on interconnected sensors in mobile devices is the center of consideration. With mobility we get *dynamism, unpredictability, faults, hand-offs, disruptions* when sensing, communicating, analyzing data, and providing energy, security, and privacy-aware mobile services. To achieve the goal, we will elaborate on IoMT challenges, design and implementation issues with respect to an integrated data cycle, starting from sensory data collection, continuing with data forwarding and delivery, to finishing with data analysis. The data cycle operations will take into account the context issues as well as the Internet access and connectivity to other cyber-physical infrastructures. Over the data cycle operations, we will consider the cross-cutting energy, security and privacy properties. In Fig. 1 we illustrate the interpreted data cycle impacted by mobility, energy, security, and privacy considerations.

The contributions of the paper are (a) the characterization of Internet of Mobile Things, their challenges and opportunities to explore new problem spaces, (b) directions to solve these challenges based on the related work and our own work, providing selective design methodologies and implementations, and (c) principles that one needs to consider and adhere to in order to have successful interactions among mobile things.

The paper is outlined as follows. In Section II, we outline the mobility challenges and opportunities that we see when considering mobile sensory data collection, exchange and analysis, as well as the energy, security and privacy challenges one has when things are moving. Section III discusses data collection from mobile devices, the design methodology and

978-1-4673-9948-7/16 $31.00 © 2016 IEEE
DOI 10.1109/IoTDI.2015.41

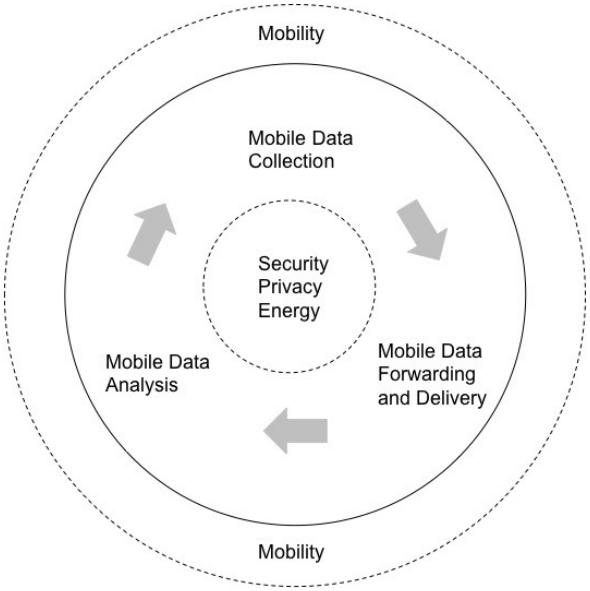



Fig. 1: Illustration of the interpreted data cycle impacted by mobility, energy, security, and privacy considerations.

implementation insights that we gained from our UIM system and experiments. Section IV presents data analysis and exchange when mobile data are collected and discusses the usage of mobile data analytics for user activity, people mobility patterns and social relation detections. Within Section V, we concentrate on one specific issue of energy management and that is the placement of energy sources for IoMT, especially in case of electric vehicles (EVs), which are our representative entities of "Mobile Things". Security, especially, the real-time authentication for EVs is discussed in Section VI, and we conclude in Section VII with lessons learned.

## II. Challenges

Within the interpreted data cycle, mobility brings challenges to the mobile sensory data collection, to the exchange of data among mobile things and computing platforms, and to the analysis of sensory data, i.e., what can the analysis help us with. Cross-cutting concerns across the entire data cycle are provisioning of energy for mobile things and security and privacy protection.

### A. Mobile Data Collection

Mobile phones and vehicles nowadays come equipped with advanced sensing and communication capabilities. These sensors can capture a wide range of information, including physical, personal, and social contextual information that can be used in data analysis and data management. However, how to leverage and manage these sensors efficiently remains challenging since each of these sensors employs a different technology with distinct tradeoffs in terms of energy consumption, connectivity, and sensing capability [6]. More importantly, the collected sensing traces are only useful if they are clean, complete, and privacy-preserved. Data collection in the context of Internet of Mobile Things (IoMT) thus become highly challenging since: (1) the wireless communication technology employed by these sensors is unreliable and error-prone, (2) continuous sensing requires a persistent supply of energy and an extensive amount of data storage. On one hand, designing a good data collection system requires extensive knowledge in sensor selection, energy management, sensing application implementation, and privacy management. On the other hand, if data collection of mobile things is done properly and effectively, it provides the fundamental building block for the success of IoMT.

In the context of IoMT, we face several challenges in the design and implementation of robust and efficient data collection systems. These challenges include:

- Selecting the right set of sensors
- Managing energy usage of sensors
- Developing sensing applications
- Preserving privacy of collected data
- Understanding people mobility and context

First, selecting the right set of sensors among all device's sensors is critical. If too many sensors are used, device's storage may run out shortly and device's power drains quickly. In contrast, if few sensors are used, the collected data might not be sufficient for data analysis. Second, managing the energy usage of sensors is highly important. In particular, setting the right scanning period to collect sufficient sensing data while preserving device's energy plays a crucial role in the design of data collection systems for IoMT. Third, developing robust sensing applications significantly impacts the quality of collected traces. Since a sensing application is essentially a software program, it competes for device's resources and its performance may be heavily influenced by other applications on the device. Implementing the sensing application so that it runs transparently and resiliently to collect prolonged data traces thus becomes fundamental for data collection. Fourth, privacy of collected data needs to be kept once the data collection system starts gathering sensing traces. How to preserve data privacy while data is processed by various components in such an universal and open environment like IoMT is critical. Finally, people mobility and context need to be well understood in the design of efficient data collection systems. In Section III, we will discuss the above mentioned challenges and selective design and implementation issues in details.

### B. Mobile Data Analytics

As sensing data are collected from mobile devices, they can be transferred to a centralized server for storage and analysis. Different from analyzing data of static sensor networks, the analysis of data from mobile devices poses a number of challenges that are centered around the *mobility* of devices:

- Mobility characterization: How to characterize the mobility of devices?
- Exploiting mobility models: How to leverage the mobility models of IoMT devices to improve the effectiveness of data analysis tasks.

We will study the challenges and selective design/implementation issues in Section IV. Here, we focus on summary of challenging issues for mobile data analysis.

The challenges with mobility characterization include defining the right metrics (i.e., representation of mobility) and analyzing the collected traces to characterize the mobility by those metrics. This is non-trivial because the collected data might be noisy and incomplete, and sometimes, lack important context information, such as location (e.g., because location sensor is turned off to save energy, or the device is indoor). In addition, the characteristics should be able to capture the realistic behaviors of people movements, which exhibit a high degree of repetition [1].

With the mobility patterns learned from characterization, the challenge becomes how to leverage those patterns to improve data analysis tasks. This requires the ability to draw the connection between the objective of each analysis task with different mobility metrics, so that the appropriate metrics are chosen as part of the analytical model for that task. For example, for the task of sensor selection, to maximize the sensing coverage, we would be interested in the mobility metrics that represent group mobility. That is because devices in the same group tend to produce highly overlapped data, and thus low collective sensing coverage. In another example, for the task of data forwarding in Delay Tolerance Networks, we would be interested in the metrics that capture contact and location regularity, since the regular contact between devices at the same location is important to design an efficient data forwarding protocol [7] [8].

### C. Energy Management

Energy management for mobile devices is a critical issue in order to accommodate the large amount of mobile things as well as the various types of mobile things. Compared to conventional energy management strategies, energy management for mobile things such as phones and electric vehicles has several distinct features including

- Energy source placement
- Energy exchange
- Cross-device energy management and monitoring

We will study the first feature in more detail in Section V. Section III includes an extensive study on energy management issues in mobile phones when performing data collection, therefore, in the rest of this section, we will focus on discussing the energy exchange challenges.

One critical challenge of energy management is to allow direct energy exchange between different devices of different users. Today it is commonly seen in airports that one charges their smartphone via a USB cable connected to their laptop. As both devices belong to the same user, there is no accounting or billing issues involved. However, with each user having access to multiple IoMT devices with different battery storage, it is likely that one sells energy directly to another in a device-to-device manner. Imagine the case where an electric vehicle runs out of battery and there is no charging station nearby. With proper support of accounting and billing protocols, the vehicle can buy electricity directly from another electric vehicle by connecting their batteries via a charging cable.

An EV can give energy not only to another EV, but also to the power grid, which is the so-called Vehicle-to-Grid (V2G) technology and has been a major research area [9], [10]. One major advantage of V2G is to smooth the load by using a collection of EVs' battery as emergency energy source orchestrated by an aggregator [11], [12]. Essentially, EVs can be viewed as mobile energy sources and part of the IoMT ecosystem. They can be used to compliment the fixed energy source placement design as we discuss in section V. In the future there might be other devices in addition to electric vehicles that can act as mobile energy sources, and we believe the current research in V2G can bring valuable lessons to the general energy exchange problem in IoMT.

### D. Security and Privacy

As an essential feature of IoMT, the devices may move and change their location. The device mobility brings unique challenges to security and privacy for IoMT compared to conventional IoT scenarios, including

- Recognizing and authenticating new devices.
- Adapting to different contexts and environments.
- Preserving location privacy.

Let us consider a typical IoT scenario of smart home appliances (TV, air-conditioner, thermometer, etc.). The smart appliances generally do not move and obtain fixed location. The appliance authentication needs to be configured only once during the initial setup. From a networking point of view, the smart home appliances constitute a static wireless network with little node churns. Now let us compare this to an IoMT scenario, where a user drives a smart vehicle on the road that communicates wirelessly with other vehicles and roadside units for collision avoidance, route suggestion, etc. The vehicle needs to constantly authenticate other vehicles as they meet on the road, which requires efficient real-time authentication as opposed to one-time initial configuration. As the vehicle moves to different areas, the environmental context may vary, e.g., wireless interference may occur when there are many other vehicles nearby communicating at the same time. The communication protocol thus needs to adapt to such changes in the context, whereas in the smart home appliance scenario the context remains mostly unchanged. The mobility of vehicles also brings location privacy into the question. The communication and authentication protocol must preserve the driver's location privacy, e.g., PKI authentication with vehicle's long-term public key will allow anyone to infer the trajectory of the vehicle by tracing the usage of the public key.

## III. Mobile Data Collection

In this section, we first discuss the design methodology in the implementation of data collection systems. We then present our implementation of a data collection system named UIM

that collected movement traces from cell phone users for six months at the University of Illinois campus.

### A. Design Methodology

How to leverage a variety of sensors to collect high quality sensing traces remains highly difficult to achieve. A collected trace is only useful if knowledge or patterns can be extracted from it. That is, the trace must be collected for an extended period of time so that data analysts can find and explain patterns derived from it. In this section, we present the design methodology of data collection systems as follows:

*a) Sensor Selection:* Selecting right sensors for the sensing task is the most critical factor [2], [13], [14]. A good sensing system should include sensors that complement each other in terms of collected data forms and formats. For example, a scanning system on the phone may not include a WiFi scanner and a GPS coordinate scanner since they both only provide location information. Further, we need to understand the tradeoff between the quality of the sensing traces one sensor collects and the amount of energy it consumes. Some sensors capture high quality sensing data but might consume too much energy for a prolonged sensing task. As a result, we may have to use sensors that provide less quality data in order to capture longer sensing traces. Although vehicles might be equipped with large storage, sensor selection still impacts the use of storage space. For example, continuous use of the camera to record video and photos on the road may fill up the vehicle's storage space quickly.

*b) Energy Management:* Once sensors are selected, the next step is to decide how frequently each sensor collects its sensing data [15]. This is crucial since it directly impacts (1) the quality of collected traces and (2) energy usage of the devices. A typical mobile phone without sensing applications may need to be recharged every two or three days. In order to obtain prolonged non-broken traces, phone carriers must remember to recharge their phones. We have learned from our real deployment, if a phone carrier does not use the phone as her daily phone, she would likely forget to recharge it. To make the phones usable for carriers, we need to ensure that sensing applications do not unreasonably drain the phones with short scanning periods. On the other hand, if we set too long scanning periods, the collected sensing data may not provide the needed granularity of information to extract adequate resource usage or people movement. At the first glance, energy consumption of sensors is not an issue with vehicles. However, since a large number of sensors is running continuously, a well-defined energy management scheme for sensors can significantly save cars power and gas.

*c) Sensing Software Development:* There are two challenges in developing sensing software on phones and vehicles. First, collecting sensing data on mobile phones and vehicles is a "best-effort" task and we always have to be prepared for the worst case scenario, i.e., implemented sensing applications may fail due to unanticipated reasons. A sensing application essentially is a software, which coexists and competes with other applications on the phones or vehicles for resources, and thus it may crash or halt at anytime. If we bundle all sensing applications of all sensors into one single sensing application, and one of sensing components crashes or one sensor fails, then it is likely that sensing applications fail altogether. If this happens, no sensing data is collected. So, sensing applications should be decoupled. Second, cell phone users or drivers install many applications on their phones and vehicles. For example, gaming and entertaining applications are favorites on phones and cars. A well-designed sensing application should incur little interference on other applications and should not interrupt the usage of users. In other words, a sensing application must: (1) start by itself whenever the device reboots for any reasons (robustness) (i.e., a phone may reboot or the dashboard in a car may reboot after a software update), (2) run in the background and not display messages on the graphic user interface (transparency), (3) keep running even if other applications halt or crash (resilience).

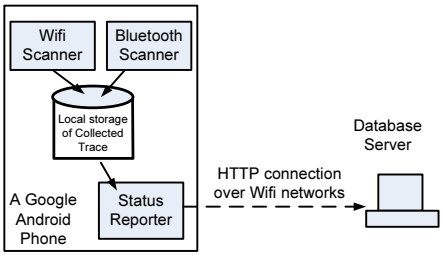


Fig. 2: UIM data collection system

*d) Privacy:* In the context of IoMT, privacy issue may arise because of the widespread use of mobile phones and vehicles since identities and locations of mobile phones and vehicles are associated with their human owners. Phones and vehicles become entities to uniquely identify their owners and their locations. As a result, identity theft becomes a major issue and identity mismatch may cause significant consequences.

*e) Mobility:* The mobility patterns and characteristics of cell phone users or vehicles can significantly impact data collection. For example, a shorter scanning period can be set to collect sensing traces if the vehicles move faster. Meanwhile, a longer scanning period can be set if the phone user performs stationary activities [16]. More importantly, since the mobility of cell phone users and vehicles is usually not known in advance, data collection in the context of IoMT is very opportunistic. That is, regardless how the sensors are selected and energy is managed, the amount of collected data depends fully on people mobility. So, the knowledge of people movement behavior can be useful in the design of data collection systems.

In the next section, we present an implementation of a mobile data collection system on Google Android phones.

### B. Implementation of Data Collection System

In this section, we present our implementation of a data collection system on Google Android phones named UIM, which stands for University of Illinois Movement. UIM addresses several challenges presented in previous section. As discussed above, the first step is to choose the sensors and we

choose to implement a WiFi scanner and a Bluetooth scanner, since WiFi scans can be used to infer location while Bluetooth scans can be used to infer social contact. These two pieces of information can be used to understand people movement behavior. Due to space limitation, we present the overview of our system here, detailed discussions and results can be found in our previous papers [17]–[20]. Figure 2 shows our system architecture, which has a WiFi scanner, a Bluetooth scanner, a database server for sensing data storage, and a Status Reporter for sensing status update. In following sections, we present the WiFi scanner and the Bluetooth scanner in detail.

*1) WiFi scanner:* The WiFi scanner has three decoupled components: a booter, a WiFi inquirer, and a WiFi receiver. Each component runs as a separate process and interacts with each other via the message passing mechanism within the Google Android phone operating system (OS). WiFi scanner runs as a background service, anytime the phone restarts, the phone OS triggers the booter, which starts the WiFi inquirer and the WiFi receiver. This design achieves robustness since anytime the phone reboots, the WiFi scanner can start its scanning work automatically. The inquirer and the receiver work in an asynchronous fashion in which the inquirer uses a request timer to periodically (i.e., every 30 minutes) issue a WiFi scanning request to the phone OS. After sending the request, the inquirer goes to sleep, and wakes up for the next request when the request timer expires. On the other hand, the receiver always sleeps and is only waken up by the phone OS whenever the WiFi scans are available for collection. Upon receiving a WiFi scan that includes a set of MACs of WiFi access points in proximity of the experiment phone, the receiver writes the WiFi scan and a timestamp to a log file, and then goes to sleep. Our design also allows the receiver to *opportunistically* receive WiFi scans, which result from other usages of WiFi connectivity, since each time the WiFi connection is initiated, a WiFi scan is performed by the phone OS. Note that keeping WiFi connection up and issuing WiFi scanning requests is much more energy-consuming than receiving WiFi scans. In order to conserve phone battery, we configure the WiFi inquirer so that it only issues scanning requests from 7AM of a day to 1AM of the next day. As a result, we can collect most of people movement while saving phone energy.

There are two reasons the WiFi scanning period is set to $30(min)$. First, our scanning system was deployed at a university campus where people usually stay in one location inside buildings for a long period (e.g., a class session is usually 50 minutes). Second, a higher WiFi scanning period may drain the phones quickly and make them unusable as daily phones for phone carriers.

*2) Bluetooth scanner:* The Bluetooth scanner has three decoupled components: a booter, a Bluetooth inquirer, and a Bluetooth receiver. Each component runs as a separate process and interacts with each other via the message passing mechanism within the Google Android phone OS. Similar to the WiFi scanner, the Bluetooth scanner is implemented as a background service. When the phone restarts, the phone OS triggers the booter, which starts the Bluetooth inquirer and the Bluetooth receiver. The inquirer and receiver work in an asynchronous fashion in which the inquirer uses a request timer to periodically (i.e., every 60(s)) issue a Bluetooth scanning request to the phone OS. After sending the request, the inquirer makes the phone discoverable by other experiment phones (so that experiment phones can scan each other), goes to sleep, and wakes up for the next request when the request timer expires. The receiver, on the other hand, sleeps and is only waken up whenever a Bluetooth scan is returned by the phone OS and ready for collection. Upon receiving a Bluetooth scan that includes a set of MACs of Bluetooth-enabled devices in proximity of the experiment phone, the receiver writes the Bluetooth scan and a timestamp to a log file, and then goes to sleep. To conserve phone energy, the inquirer is configured to only issue scanning requests from 7AM of a day to 1AM of the next day. As a result, we can collect most of people movement while saving phone energy.

*3) Collected Sensing Traces:* Table I summarizes major statistics of the sensing traces collected by the UIM system. Specifically, from March 2010 to August 2010, we conducted three rounds of experiments with 123 participants at the University of Illinois campus. Our participants included grads, undergrads, faculties, and staffs. The first experiment lasted 19 days, the second was 38 days, and the third was 85 days. The number of scanned WiFi MACs and Bluetooth MACs of the third experiment were fewer than the second experiment (although the third experiment was much longer) since the third experiment was conducted during the summer break with fewer classes and students on campus. Our traces were the most detailed traces collected in the university campus [20].

| **Overall Characteristics** | | | |
|---|---|---|---|
| Number of phones (participants) | 28 | 79 | 16 |
| Length of experiment (day) | 19 | 38 | 85 |
| Bluetooth Scanning Period (s) | 60 | 60 | 60 |
| WiFi Scanning Period (m) | 30 | 20 | 30 |
| Number of Scanned BT MACs | 8508 | 17080 | 7360 |
| Number of Scanned WiFi MACs | 7004 | 29324 | 6822 |

TABLE I: Overall characteristics of our collected traces

*4) Impact of Energy Usage on Amount of Collected Data:* In this section, we investigate the impact of energy usage on data collection. Specifically, we study changes in the number of collected WiFi MACs when we vary the scanning period (or scanning frequency) of the WiFi scanner. We have a participant carry the phone with an implemented WiFi scanner for a week (or seven days) and the scanning frequency is set to 5 minutes. After one week, we receive the dataset $D_5$ of the 5 minute scanning frequency. This is the largest dataset and then we create smaller datasets with longer "artificial" scanning frequencies of 15, 30, 60, 120 minutes from $D_5$. For example, the dataset $D_{15}$ of the scanning frequency of 15 minutes is created by taking the $i^{th}$, $(i+3)^{th}$, and $(i+6)^{th}$, and so on scanning records of $D_5$, since records in $D_{15}$ is

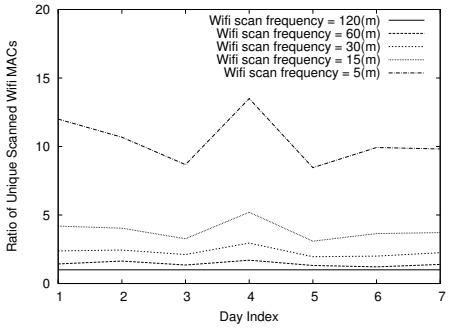



Fig. 3: Impact of Scanning Period on Collected Data

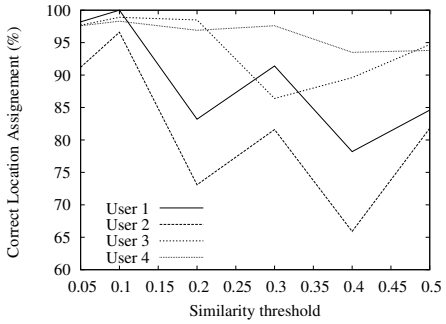



Fig. 4: Results on inferring location by clustering WiFi records

15 minutes apart while records in $D_5$ is five minutes apart. The dataset $D_{120}$ is the smallest dataset since it is derived from the longest frequency. We use $D_{120}$ as the baseline and for each day (of seven days), we calculate the ratios of $\frac{D_k}{D_{300}}$, with $k \in \{5, 15, 30, 60, 120\}$ and plot these ratios in Figure 3. The x-axis of the figure is the index of day in the one week experiment and the y-axis is the ratio $\frac{D_k}{D_{300}}$. This figure shows a clear tradeoff between the scanning frequency and the amount of collected sensing data. A shorter scanning period will collect bigger traces. In other words, if more energy is used for scanning, we will collect larger traces. So, the scanning period should be set carefully so that phones can perform prolonged experiment while collecting acceptable traces.

## IV. Mobile Data Analysis

In this section, we present our design methodology and implementations of mobility characterization, and our approach to leverage mobility to improve mobile data analysis tasks.

### A. Mobility Characterization

*1) Design Methodology:* The main challenges in mobility characterization are to define the right metrics and to analyze the collected traces towards mobility characterization by those metrics.

In terms of the metrics, we focus on the contextual information that help define the movement of mobile device users, including temporal, spatial, and social context. By capturing those contexts, we will be able to answer questions about the mobility patterns of mobile devices: Where does the device move over time?, What are the most regular visit locations?, or Which devices it interacts with most frequently? Among those information, location is the required information that a characterization study must obtain, since knowledge of where people visit is fundamental to obtain movement patterns. In case location information is not available (e.g., GPS sensor is turned off to save energy, or when the device is indoor), we need to infer the locations of devices based on other non-spatial information, or *location profiling*.

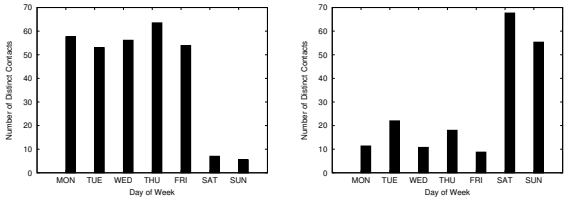
In terms of mobility characterization, we believe a good characterization study should be able to capture contact patterns, stay duration at a location, and grouping behavior of people movement. Knowledge of who a person meets at a certain time (i.e., contact) allows us to understand the social interactions and contact patterns, which can be a key factor in social science studies and the design of efficient message forwarding schemes for mobile networks [7]. Given the stay duration at locations, we can estimate the arrival and departure time at locations, which is essential for many applications such as traffic monitoring, social network analysis, urban planning. Characteristics of contact group formed by co-located people, if available, could be used to enrich collected sensing data (e.g., inferring missing contacts), or infer new knowledge for sensor selection.

*2) Implementation of Mobility Characterization on UIM Traces:* In this section, we first present our implementation on acquiring location information from non-spatial data, and then, describe our findings on mobility characterization for in-door environments.

In terms of location profiling, from the collected traces of Bluetooth and WiFi scans, we infer location information by clustering the WiFi records (i.e., records of WiFi access point SSID detected by mobile devices overtime) [17], [18]. Specifically, we define location as a unique set of WiFi access points, or a WiFi record. Since the WiFi scan results from different devices are not always consistent, even at the same location, we first construct a similarity graph of WiFi scan records (the more overlap between two records, the more similar they are) and then perform clustering over the records. Each cluster in the final result represents a physical location. Figure 4 presents the accuracy of our results on inferring locations by clustering WiFi scan records for different users using different similarity thresholds.

In terms of mobility characterization, by analyzing collected traces of Bluetooth contacts and aggregating them over time, we are able to identify distinctive contact patterns of users [14]. Figure 5a shows the first contact pattern in which people usually have a considerably higher number of contacts during the weekdays than the weekends. This is the most common contact pattern found in our sensing traces since most people perform the casual routines at work for the weekdays when they make contacts with many more people. In contrast, Figure 5b shows an opposite (and less popular) contact pattern in which people make more contacts during the weekends than the weekdays.

In terms of stay duration and location regularity, our analysis




(a) Fewer contacts at the weekend. (b) More contacts at the weekend.

Fig. 5: Distinctive contact patterns.

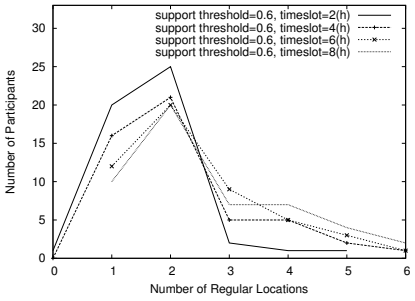



Fig. 6: Location regularity by different frequency thresholds.

[14] helps answer the question: Do people visit locations regularly for their daily activities? A location is regular if the number of people at that location during a time period exceeds a certain regularity threshold. Figure 6 shows the regularity of locations with time period of 6 hours and different regularity threshold. The results show that most people have at least two regular locations. This is consistent with the results of previous work, which have shown that people spend most of their time at a few places, such as their home and work locations [1] [3].

For contact group behavior, our results (Figure 7) show that people rarely form large contact groups during their daily activities (i.e., 90% of groups have the size of 6 or smaller). This should take into account that the collected data [20] are from a university campus. Algorithms in multi-casting, content distribution, or DTNs could benefit greatly from these results.

### B. Exploiting Mobility Models

*1) Design Methodology:* The results of mobility characterization help us improve the performance of various data

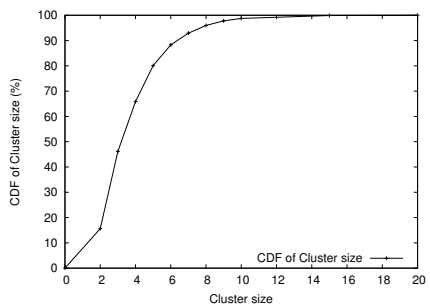
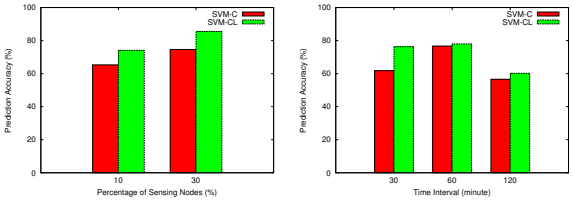



Fig. 7: Contact groups.




(a) Impact of number of sensors. (b) Impact of time interval.

Fig. 8: Predicting missing contacts.

analysis tasks.

First, to improve the completeness of collected data, we leverage the contact patterns and group mobility behaviors to recover the contacts that have been missing from the collected traces [14] (i.e., due to sensing errors or limited number of sensing devices).

Second, with more complete traces and the understanding of people mobility, we are able to predict people's future movements [17], [18].

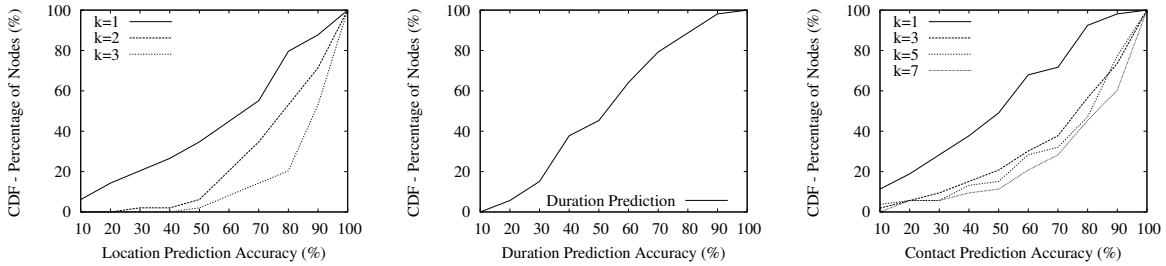
Third, our understanding of mobility patterns helps us to improve sensor selection to maximize the sensing coverage [21], and improve message delivery in mobile peer-to-peer networks [8].

*2) Implementation: Usage of Mobility Models:*

*a) Predicting missing contacts:* To improve the completeness of collected traces, we leverage contact patterns, location information of devices, and the observed contacts to build binary classifiers (using Support Vector Machine (SVM)) and to classify whether a contact between two devices exists or not. The results (Figure 8) show that the model that uses mobility patterns (i.e., SVM-CL) outperforms the model that only uses the contact statistics (i.e., SVM-C) for different sensing intervals and different number of sensing devices.

*b) Predictive models of future movement:* We exploit the regular patterns of people movement learned from mobility characterization to predict the future movements [17], [18]. Particularly, we train three supervised machine learning based predictive models using Naive Bayesian technique, including location predictor, stay duration predictor, and contact predictor. We then evaluate these predictors with three different datasets. The experiment results (Figure 9) show that our predictors perform well and provide accurate prediction on location (i.e., Figure 9a), stay duration (i.e., Figure 9b), and social contacts (i.e., Figure 9c).

*c) Sensing devices selection:* From the insights of the contact group and location popularity characteristics, we implement a context-aware sensing devices selections [21] to maximize collective sensing coverage in opportunistic mobile social networks. Our results (Figure 10) show that, by leveraging spatio-temporal contexts from the observed mobile data traces, our approach (denoted as HCONTEXT) is able to assign the sensing tasks to the group of devices to achieve better collective sensing coverage, compared with other optimization approaches (i.e., GREEDY for greedy coverage selection, and RANDOM for random selection of sensing devices). Details




(a) Location prediction. (b) Location stay duration prediction. (c) Contact prediction.

Fig. 9: Future movements prediction results.

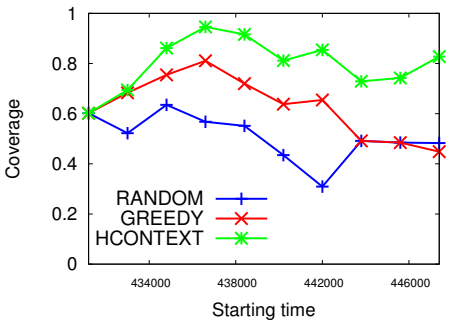
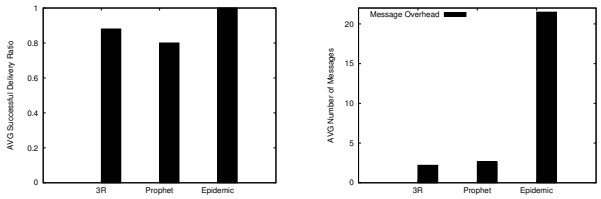



Fig. 10: Sensing coverage comparison




(a) Average Successful Delivery Ratio (b) Average Message Overhead

Fig. 11: Comparison of 3R with Epidemic and Prophet routing protocols.

of our approach can be found in [21].

*d) Content Distribution:* Mobility characteristics and models, learned from characterization studies, can be used to improve message delivery in mobile peer-to-peer networks [8] [22] [7] [23]. Specifically, we first analyze UIM traces and then design an efficient routing protocol named 3R that exploits regular contact patterns found in the mobility traces for message delivery. Figure 11 compares 3R and two other state of the art message forwarding protocols, named Prophet [7] and Epidemic [22]. Our evaluation shows that 3R outperforms Prophet in successful message delivery ratio while minimizing message overhead. Details of our protocol design can be found in [8].

## V. Energy Management

Since IoMT devices are powered by electricity, the first challenge of energy management for IoMT is to deliver energy to the device. One crucial problem of energy delivery is the energy source placement. For example, today users might experience difficulty in finding energy sources in an airport to charge their smartphones. As users use more and more IoMT devices that need charging, the placement of energy sources has increased impact on the usability of mobile devices.

The most notable mobile devices that can be affected by the placement of energy sources are electric vehicles (EVs). Compared to conventional combustion engine vehicles, electric vehicles have much shorter range, and typically require daily charging. In this section, we focus on discussing the energy source placement issues for electric vehicles.

### A. Charging Facilities

Charging station is one type of widely adopted charging facilities for electric vehicles. Charging stations charge electric vehicles similarly to gas stations in the way that vehicles come into the stations to get served and stay for a certain amount of time to get their batteries charged to a satisfactory level. However, major concerns about charging stations are electrocution and charging stations becoming frozen on vehicles in extreme weather [24]. This facilitates the development of static and dynamic wireless charging pads. And the placement of charging stations and wireless charging pads has an important impact on both the driver's convenience and the traffic flow.

Since the wireless charging pads are not widely deployed yet, despite the major concerns of charging stations, charging stations are the most widely adopted charging facilities on the road network for electric vehicles. The charging stations must be placed not too far away from each other to ensure good coverage, and not too close to each other to avoid causing traffic congestion in case many electric vehicles choose to charge in the same area. The charging stations are placed normally at intersections of road networks or points of interests in cities. These locations are typically modeled as nodes of a network graph. When planning charging stations, the design issues and considerations are

- Determining the locations for placing charging stations.

- Determining the number of charging servers at each charging station. Note that charging servers are the access handles for electric vehicles to connect to the energy source. Charging servers work similarly to the refueling pumps at gas stations in the way that each electric vehicle needs to obtain a charging server to get charged. And each charging station could have several charging servers in order to minimize the waiting time of electric vehicles by charging multiple electric vehicles at the same time.
- The workload of charging stations also needs to be taken consideration and a load balancing strategy is needed in order to balance the energy load across the power grid.

### B. Wireless Charging

As described in the previous subsection, wireless charging pads are another type of charging facilities for electric vehicles. Electric vehicles can get charged by parking over a static wireless charging pad. They can also get charged dynamically by driving over the wireless charging pads. Dynamic charging, using wireless charging pads, has been studied in recent years [25]–[29]. In dynamic charging of electric vehicles, the magnetic induction between the charging pads installed under the road and the receiving coils attached to the EV's battery automatically charges the EV as it moves over the charging pads. Each charging pad is typically short (e.g., 30-50 cm), and a charging section of several kilometers consists of a series of charging pads placed close to each other (e.g., 50 cm away). The advances of dynamic charging allow EV's battery to be charged while moving over wireless charging pads. But the advances of dynamic charging also complicate the energy source placement problem.

The placement of charging pads depends on the models of electric vehicles. Different models share various features such as battery capacity, max charging rate and miles of charging per hour. And these features lead to different maximum driving distances, required charging times, etc. It also heavily depends on the traffic flow densities on the road network. Traffic flow density is defined as the number of electric vehicles per unit length of the road link. Placing charging pads along the road links that have heavy traffic flows helps to maximize the amount of electric vehicles traveling on the roads. We also need to consider the impact of the traffic flow patterns. For example, for traffic flows during peak hours, turning the charging pads on during the peak hours while keeping them off for the rest of the day may help saving energy compared to turning the pads on for the whole day.

The placement of static wireless charging pads is similar to the placement of charging stations which is discussed in Section V-A. Static wireless charging pads are normally placed at points of interests and each service area (i.e. charging spot) includes several charging pads to support charging multiple electric vehicles at the same time. However, dynamic wireless charging pads are placed under the roadbed and require that EVs travel a certain distance to get charged. The design issues for dynamic wireless charging pads include

TABLE II: Maximum flow charged under various situations

| # pad | # station | Configuration | Volume (veh/hr) |
|---|---|---|---|
| 3 | 0 | L4, L5, L10 | 3515.1 |
| 2 | 1 | L4, L5, N1 | 2309.1 |
| 1 | 2 | N1, N2, L5 | 2726.9 |
| 0 | 3 | N1, N2, N4 | 1692.2 |

- Determining which road links to equip with the dynamic wireless charging pads.
- Deciding how many charging pads should be placed on a certain road link.
- Determining when to turn on and off the charging pads.

### C. Implementation of Energy Source Placement Model

In this subsection we describe our initial design and simulation towards solving the source placement for charging stations and wireless dynamic charging pads for electric vehicles.

The design in [30] focuses on placement of both charging stations and charging pads. Several assumptions are made to simplify the implementation:

- We assume that charging pads are always turned on.
- Every road link is treated as one entity and is not further segmented into smaller sections. It means that a road link gets charging pads or it gets none.
- We assume that after traveling on the road links which have charging pads, vehicles will be charged to full battery status.[1]

When considering allocating charging stations, we adopt the Flow Refueling Location Model (FRLM) proposed in [31]. FRLM is a flow-based location-allocation model which aims at finding optimal locations for refueling stations.

The placement of energy charging stations and wireless pads for electric vehicles problem is formulated as an optimization problem and we simulate the model on a 9-node center-formed sample network as depicted in Figure 12 of which the feature of traffic flows is similar to the city Berlin in Germany. It means that the center node/district attracts and generates the largest amount of traffic flows that travel between the center node and its surrounding nodes.

We test our allocation model given different charging facilities and the evaluation results are shown in Table II. For example, when allocating 2 charging stations and 1 road link with charging pad, the maximum amount of traffic flows we are able to charge is 2309.1 (veh/hr). The evaluation results indicate that placing charging pads on 3 road links doubles the amount of vehicles being charged in comparison to placing 3 charging stations only. The bold lines in Figure 12 indicate the selected links for placing charging pads. The selected links are the links that have the top amount of traffic flows of the road network and assigning charging pads to these links helps to satisfy the charging needs of these traffic flows first.

[1]This assumption requires very long road links, which is not very realistic. In our future work we will investigate pratial charging with energy source placement.

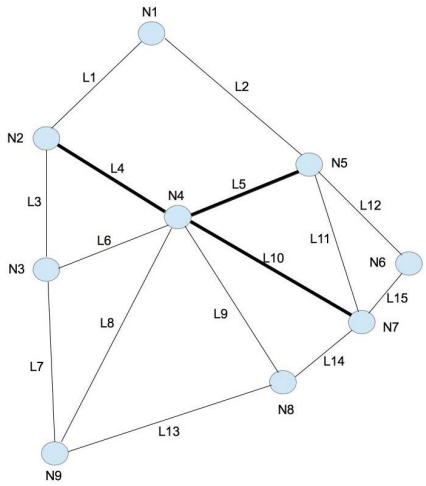



Fig. 12: Sample network with 9 nodes, where nodes (e.g., $N1, N2$) represent road intersections, and lines (e.g., $L1, L2$) represent road links. Bold lines indicate that 3 links are selected to place dynamic wireless charging pads.

## VI. Security and Privacy

In Section II-D, we have briefly discussed the security and privacy challenges brought by the concept of IoMT. In this section we use authentication as an example, discuss various challenges of authentication for IoMT devices, and review a recent authentication protocol for dynamic charging of electric vehicles to illustrate the impact of mobility on protocol design and implementation.

### A. Challenges for Authentication of IoMT devices

Authenticating the identity of devices is by no means a new problem in security research. Consider an IoT scenario, where the doorbell has a camera that connects to the living room TV through the in-house WiFi router. Since neither the doorbell nor the TV are likely to move, the wireless connection and the authentication between the doorbell and the TV only need to be configured once during the initial setup. What makes mobile device authentication a new challenge is the fact that (i) the device changes its location as the user moves; and (ii) it constantly meets new other IoMT-enabled devices, as opposed to having a fixed list of neighbors which it has learned during its pre-configuration.

While authentication in vehicular network has been extensively studied in the research community [32]–[37], we want to emphasize that they constitute only a small subset of applications of IoMT. In particular, most V2V authentication approaches focus on authenticating the safety message that has a fixed content (location and speed) and fixed broadcast frequency (every 100 milliseconds) according to the IEEE 802.11p standard, and most Vehicle-to-Infrastructure (V2I) authentication solutions focus on authentication between vehicles and roadside units. It is easy to imagine an IoMT scenario that goes beyond the current focus of V2V and V2I authentication: the vehicle may communicate with street-side stores to receive price information, share multimedia content with other vehicles, or communicate with pedestrians carrying IoMT-enabled devices for collision avoidance. Apparently vehicles, pedestrians, and streetside stores have different mobility patterns, and an authentication framework for IoMT is needed that is able to authenticate different types of devices with different mobility patterns.

Let us consider an example from vehicule-to-vehicle (V2V) communication, where vehicles periodically broadcast their own speed and location to help avoid collision with other vehicles. When a vehicle receives a message containing the speed and location information, it must verify that the message is indeed generated by another vehicle nearby, instead of a fake message generated by an attacker trying to mislead the driver into changing its speed. In this V2V authentication scenario, the challenge is that a vehicle needs to constantly authenticate new vehicles, and depending on the speed of the traffic flow, the contact time with a new vehicle is small and the authentication must be completed within milliseconds.

Another challenge for authentication in IoMT scenario is that the mobile device may need to authenticate with other mobile devices very frequently. Recall the dynamic charging scenario for electric vehicles (EVs) introduced in Section V-A. When the EV is moving at high speed (e.g., 70 mph), it encounters and authenticates with a new charging pad around every 20 milliseconds, and the authentication must complete within the first few of the 20 milliseconds so that the rest can be used to charge the EV's battery. This makes it very challenging to design the authentication protocol.

### B. Design of Portunes+ Authentication Protocol

We have designed a solution for the dynamic charging authentication problem [38]. Our authentication design, called Portunes, adopts a key-predistribution approach where session keys are generated and pre-distributed to charging pads prior to the actual authentication. We have further improved our design and proposed Portunes+ by including an implicit authentication protocol that allows the charging pads to share authentication results with each other and effectively reduce the required authentication frequency [39].

Portunes+ involves three different entities: the Charging Service Provider (CSP) that the EV subscribes to, the Pad Owner (PO) that operates the dynamic charging section, and the EV. The intuition behind dividing the authentication into two phases also comes from an observation of the mobility pattern of vehicles: statistics have shown that most vehicles (except for trucks) are parked during the night (e.g., between 1 am and 6 am). From the authentication protocol's point of view, when the EV is parked, it is idle in that it will not interact with the charging pads under the road to charge its battery. This idle period thus provides an opportunity where cryptographic operations can be performed in preparation for future use.

In Fig. 13 we illustrate the major steps in Portunes+. In the key pre-distribution phase, the CSPs generate the key sets and send them to the POs, which in turn disseminate the key

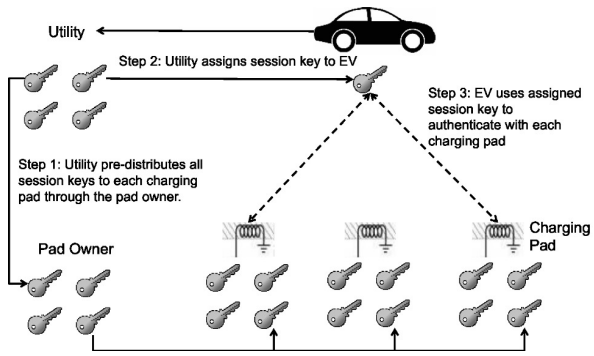



Fig. 13: Overview of Portunes+ authentication

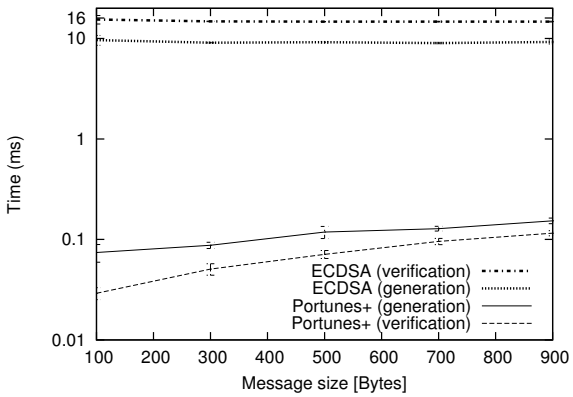



Fig. 14: Generation and verification time of authentication message using Portunes+ and ECDSA vs. message size. Error bars indicate 95% confidence intervals. The evaluation is done on Raspberry Pi 2 Model B.

sets to each charging pad. In the authentication step, the CSPs allocate keys and pseudonyms to EVs before they enter the charging section, and the EVs authenticate with each charging pad encountered using the assigned key. The true identity of the EV is not revealed to the charging pads during the authentication. Since the session key assigned to the EV has already been pre-distributed to the charging pads, the EV can immediately start using the assigned session key for mutual authentication with the charging pads without additional key negotiation.

### C. Implementation and Results

We have implemented Portunes+ in C++ using Crypto++ 5.6.2 library, and evaluated its performance on Raspberry Pi 2 Model B platform. Raspberry Pi is a portable general computing platform featuring a 900 MHz Quad-core CPU and 1 GB RAM, and costs $35 (USD) at the time of writing. We choose to evaluate Portunes+ on Raspberry Pi because we think future EVs will be equipped with equivalent or better computational resources. As shown in Fig. 14, the authentication message generation and verification of Portunes+ are orders of magnitude faster compared to Elliptic Curve Digital Signature Algorithm (ECDSA) currently suggested by the IEEE 802.11p standard.

One important lesson we learned is that the mobility pattern of the IoMT devices in question plays an important role in designing the protocol. The reason why Portunes+ outperforms ECDSA in real-time authentication speed is that Portunes+ utilizes the idle period during which the EV is parked to perform computationally intensive operations, and only uses lightweight cryptographic operation during real-time authentication. This two-phase design choice comes from the observation on the vehicle's mobility pattern, i.e., most sedan vehicles are parked during the night.

## VII. Conclusion

In this paper, we have discussed Internet of Mobile Things with variety of themes ranging from data collection, analysis, exchange to energy management and security and privacy of mobile things. In each of these themes, one can draw many lessons learned. We want to highlight some of them.

First, in *data collection*, mobility of things such as phones and vehicles impacts several important relations: (a) relation between number of sensors used during data collection, energy usage, and storage usage, i.e., if number of sensors goes up in a mobile device, energy usage goes up and data collection requires more storage space; (b) relation between data collection, energy management and data analysis, i.e., if one collects more data, more energy is being spent, but also better data analysis can be done learning more detailed patterns such as mobility patterns, usage patterns, social context patterns, and other patterns of mobile devices; (c) relation between data collection and privacy; i.e., if one collects private data, one needs to provide privacy-preserving algorithms for mobile devices; (d) relation between data collection and data quality, i.e., since mobile data collection is opportunistic, how much data one collects (duration and frequency of data collection) impacts the data quality implicitly.

Second, during *data analysis* and delivery, one has to pay attention to the following issues: (a) relation between data selection for analysis and mobility, i.e., mobility will impact the data selection for analysis since if one chooses data that is erronous during high mobility speeds, analysis will be highly erronous as well. (b) relation between data analysis, security, privacy and energy; i.e., the accuracy of analysis and the level of security/privacy very much depend on the energy availability on a mobile phone and vice versa.

Third, in our *energy management* considerations, two lessons learned came out: (a) strong assumptions on the mobility of devices make the modeling and analysis of energy placement easier, but one needs to relax the strong assumptions to encompass more realistic scenarios; (b) relation between energy placement, mobility patterns, and data collection and analysis is of importance since if one understands mobility patterns of devices, one can better design placement of energy sources, and in order to gain accurate mobility patterns, one needs to do data collection and analysis from devices to get

their individual locations and energy usage.

Fourth, *security* is very much impacted by the mobility since (a) mobility means adaptation and adaptation means design of security protocols that accept continuous changes in key management, exchange of credentials, authentication algorithms and other parts of the security and privacy frameworks; (b) relation between data analysis and security will impact predictions in mobility patterns which again can yield better key management and stronger authentication via a two-factor authentication.

In summary, even though research around Internet of Mobile Things may happen along the above discussed themes separately, it is very important to stress that all of these themes, i.e., data collection, analysis, exchange, energy management, and security and privacy, *must* be considered together. Only an *integrated approach* towards IoMT will be successful if we want to see Internet of Mobile Things developed and deployed broadly.

## REFERENCES


[1] M. C. Gonzalez, C. A. Hidalgo, and A.-L. Barabasi, "Understanding individual human mobility patterns," *Nature*, vol. 453, no. 7196, pp. 779–782, 2008.

[2] T. M. T. Do and D. Gatica-Pereza, "The places of our lives: Visiting patterns and automatic labeling from longitudinal smartphone data," *IEEE Transactions on Mobile Computing*, vol. 13, 2014.

[3] S. Isaacman, R. Becker, R. Cáceres, S. Kobourov, M. Martonosi, J. Rowland, and A. Varshavsky, "Identifying important places in peoples lives from cellular network data," in *Pervasive computing*. Springer, 2011, pp. 133–151.

[4] G. Mohimani, F. Ashtiani, A. Javanmard, and M. Hamdi, "Mobility modeling, spatial traffic distribution, and probability of connectivity for sparse and dense vehicular ad hoc networks," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 4, pp. 1998–2007, May 2009.

[5] F. Calabrese, M. Diao, G. Di Lorenzo, J. Ferreira, and C. Ratti, "Understanding individual mobility patterns from urban sensing data: A mobile phone trace example," *Transportation research part C: emerging technologies*, vol. 26, pp. 301–313, 2013.

[6] C. C. Aggarwal and A. Sheth, "The internet of things: A survey from the data-centric perspective." Springer, 2013.

[7] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: social-based forwarding in delay tolerant networks," in *MobiHoc*, 2008.

[8] L. Vu, Q. Do, and K. Nahrstedt, "3r: Fine-grained encounter-based routing in delay tolerant networks," in *Proceedings of International Symposium on a World of Wireless, Mobile and Multimedia Networks(IEEE WoWMoM)*, 2011.

[9] J. Pinto, V. Monteiro, H. Goncalves, B. Exposto, D. Pedrosa, C. Couto, and J. Afonso, "Bidirectional battery charger with grid-to-vehicle, vehicle-to-grid and vehicle-to-home technologies," in *Industrial Electronics Society, IECON 2013 - 39th Annual Conference of the IEEE*, Nov 2013, pp. 5934–5939.

[10] M. Yilmaz and P. Krein, "Review of the impact of vehicle-to-grid technologies on distribution systems and utility interfaces," *Power Electronics, IEEE Transactions on*, vol. 28, no. 12, pp. 5673–5689, Dec 2013.

[11] C. Liu, K. Chau, D. Wu, and S. Gao, "Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies," *Proceedings of the IEEE*, vol. 101, no. 11, pp. 2409–2427, Nov 2013.

[12] P. Dutta and A. Boulanger, "Game theoretic approach to offering participation incentives for electric vehicle-to-vehicle charge sharing," in *Transportation Electrification Conference and Expo (ITEC), 2014 IEEE*, June 2014, pp. 1–5.

[13] T. M. T. Do and D. Gatica-Pereza, "Where and what: Using smartphones to predict next locations and applications in daily life," *Pervasive and Mobile Computing Journal*, vol. 12, pp. 79–91, 2014.

[14] L. Vu, P. Nguyen, K. Nahrstedt, and B. Richerzhagen, "Characterizing and modeling people movement from mobile phone sensing traces," *Pervasive and Mobile Computing Journal*, vol. 17, pp. 220–235, 2015.

[15] Y. Chon, E. Talipov, H. Shin, and H. Cha, "Mobility prediction-based smartphone energy optimization for everyday location monitoring," in *Proceedings of SenSys*, 2011, pp. 82–95.

[16] N. Ravi, N. Dandekar, P. Mysore, and M. L. Littman, "Activity recognition from accelerometer data," in *AAAI*, 2005.

[17] L. Vu, Q. Do, and K. Nahrstedt, "Jyotish: Constructive approach for context predictions of people movement from joint wifi/bluetooth trace," *Pervasive and Mobile Computing Journal*, vol. 6, pp. 690–704, 2011.

[18] ——, "Jyotish: A Novel Framework for Constructing Prediction Model of People Movement from Joint Wifi/Bluetooth Trace," in *Proceedings of Percom*, 2011.

[19] L. Vu, "Characterizing and leveraging people movement for content distribution in mobile peer-to-peer networks," Ph.D. dissertation, University of Illinois, 2010.

[20] L. Vu, K. Nahrstedt, S. Retika, and I. Gupta, "Joint Bluetooth/Wifi scanning framework for characterizing and leveraging people movement in university campus," in *Proceedings of MSWiM*, 2010.

[21] P. Nguyen and K. Nahrstedt, "Context-aware crowd-sensing in opportunistic mobile social networks," in *Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on*. IEEE, 2015, pp. 477–478.

[22] F. Li and J. Wu, "Localcom: A community-based epidemic forwarding scheme in disruption-tolerant networks," in *SECON*, 2009.

[23] A. Lindgren, A. Doria, and O. Scheln, "Probabilistic routing in intermittently connected networks," in *Mobihoc*, 2003.

[24] H. Wu, A. Gilchrist, K. Sealy, P. Israelsen, and J. Muhs, "A review on inductive charging for electric vehicles," in *Electric Machines Drives Conference (IEMDC), 2011 IEEE International*, May 2011, pp. 143–147.

[25] G. Covic and J. Boys, "Modern Trends in Inductive Power Transfer for Transportation Applications," *IEEE ESTPE*, 2013.

[26] S. Lee, J. Huh, C. Park, N.-S. Choi, G.-H. Cho, and C.-T. Rim, "On-Line Electric Vehicle using inductive power transfer system," in *ECCE'10*.

[27] S. Ahn and J. Kim, "Magnetic field design for high efficient and low EMF wireless power transfer in on-line electric vehicle," in *EUCAP '01*.

[28] H. Wu, A. Gilchrist, K. Sealy, P. Israelsen, and J. Muhs, "A review on inductive charging for electric vehicles," in *IEMDC*, May 2011.

[29] "Stanford report," http://news.stanford.edu/news/2012/february/wireless-vehicle-charge-020112.html.

[30] S. Chang, H. Li, and K. Nahrstedt, "Charging facility planning for electric vehicles," in *Electric Vehicle Conference (IEVC), 2014 IEEE International*, Dec 2014, pp. 1–7.

[31] M. Kuby and S. Lim, "The flow-refueling location problem for alternative-fuel vehicles," *Socio-Economic Planning Sciences*, vol. 39, no. 2, pp. 125 – 145, 2005.

[32] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," in *SECON '09*.

[33] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Flooding-resilient broadcast authentication for VANETs," in *ACM MobiCom*, 2011.

[34] H. Li, G. Dán, and K. Nahrstedt, "Lynx: Authenticated Anonymous Real-Time Reporting of Electric Vehicle Information," in *IEEE International Conference on Smart Grid Communications (SmartGridComm), 2015*.

[35] ——, "Proactive Key Dissemination-Based Fast Authentication for In-Motion Inductive EV Charging," in *IEEE International Conference on Communications (ICC), 2015*.

[36] J. Almeida, S. Shintre, M. Boban, and J. Barros, "Probabilistic key distribution in vehicular networks with infrastructure support," in *Global Communications Conference (GLOBECOM), 2012 IEEE*, Dec 2012, pp. 973–978.

[37] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An Efficient Message Authentication Scheme for Vehicular Communications," *Vehicular Technology, IEEE Transactions on*, vol. 57, no. 6, pp. 3357–3368, Nov 2008.

[38] H. Li, G. Dán, and K. Nahrstedt, "Portunes: Privacy-preserving fast authentication for dynamic electric vehicle charging," in *IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014*.

[39] ——, "Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging," in *IEEE Transactions on Smart Grid (to appear)*.