People-Centric Urban Sensing: Security Challenges for the New Paradigm

Peter Johnson Apu Kapadia David Kotz
Nikos Triandopoulos

Institute for Security Technology Studies*
Dartmouth College
Hanover, NH USA

Dartmouth Computer Science Technical Report TR2007-586
February 2007

Abstract

We study the security challenges that arise in *people-centric urban sensing*, a new sensor-networking paradigm that leverages humans as part of the sensing infrastructure. Most prior work on sensor networks has focused on collecting and processing ephemeral data about the environment using a static topology and an application-aware infrastructure. People-centric urban sensing, however, involves collecting, storing, processing and fusing large volumes of data related to every-day human activities. Sensing is performed in a highly dynamic and mobile environment, and supports (among other things) pervasive computing applications that are focused on enhancing the user's experience. In such a setting, where humans are the central focus, there are new challenges for information security; not only because of the complex and dynamic communication patterns, but also because the data originates from sensors that are carried by a person—not a tiny sensor thrown in the forest or mounted on the neck of an animal. In this paper we aim to instigate discussion about this critical issue—because people-centric sensing will never succeed without adequate provisions for security and privacy. To that end, we outline several important challenges and suggest general solutions that hold promise in this new paradigm of sensor networks.

*This research program is a part of the Institute for Security Technology Studies, supported by Grant number 2005-DD-BX-1091 awarded by the Bureau of Justice Assistance, by NIST under award 60NANB6D6130 from the U.S. Department of Commerce, and by the Institute for Information Infrastructure Protection (I3P) under an award from the Science and Technology Directorate at the Department of Homeland Security. Points of view or opinions in this document are those of the authors and do not represent the official position or policies of the United States Department of Justice, the U.S. Department of Commerce, or the U.S. Department of Homeland Security.

1 Introduction

Sensor networks provide tremendous potential for information collection and processing in a variety of application domains. The first generation of sensor-network scenarios include stationary devices sensing ephemeral features of the environment around them. In this paper we focus on a new generation of sensor networks, those aimed at everyday applications in daily life and at the use of "people-centric" devices in dense urban environments. *People-centric urban sensing* has been introduced [6] as a term that describes this new paradigm: small computational devices, carried by individuals in their daily activities, sense information directly or indirectly related to human activity, as well as aspects of the environment around them.

This new kind of sensor network is based on a different set of assumptions and trade-offs than in much of the prior work on sensor networks, requiring new thinking about the communications infrastructure. Likewise, these new capabilities and architectures create new needs and require new solutions for information security. First, the likely applications deal with highly sensitive or private information, requiring a deeper attention to privacy and anonymity than in most prior work. Second, different assumptions about device and network capabilities (including high mobility, opportunistic networking, strong but not continuous connectivity, and relatively plentiful power) lead to different opportunities for sensor-network architecture and push different security solutions. For example, previous work has focused on security solutions for resource-constrained devices [44, 65], secure routing techniques for static sensor networks [11, 34, 64] and secure data collection and aggregation in static and fixed tree topologies [8, 47]. Furthermore, since sensors could fall into the hands of adversaries, attention was paid to secure key management and distribution schemes that could tolerate compromise [28, 30, 63]. Given the trend toward urban-sensing applications and the potential for people-centric sensors, the time is ripe to explore new security and privacy challenges. In this setting, sensor devices will (i) be highly mobile, so existing security solutions that assume fixed topologies cannot be employed; (ii) have limited resources, but not severely so; thus new cryptographic techniques can be employed (e.g., we may assume that public-key cryptography will not significantly degrade a sensor node's lifetime [46]); and, critically, (iii) most sensors will be carried by people, thus introducing critical privacy concerns as well as new adversarial threat models.

This paper contributes to the discussion by surveying these security and privacy challenges, and identifying some key solution concepts. We hope this work will instigate further work on this critical topic.

In Section 2 we overview urban sensing and identify the key features and assumptions driving a need for new solutions. We discuss the applications enabled by this form of sensor network in Section 3. In Section 4, we describe what we believe to be the new challenges and discuss some conceptual solutions. We summarize the paper in Section 5.

2 Urban Sensing

Wireless sensor networks provide a structure for gathering data on scales and in environments previously unattainable. In 2002, the Great Duck Island Experiment [40] successfully

demonstrated both of these characteristics by dropping a large number of small wireless sensors on a remote island to study the nesting habits of the Leach's Storm Petrel seabird. Other projects followed, such as the Macroscope in the Redwoods [51] and a counter-sniper system [49], which continued to demonstrate the viability of the field.

Forests and battlegrounds, however, are not the only interestingly "sensable" locales: new research is proceeding on sensing in urban environments. These environments present a potentially much larger coverage area than a single redwood tree, or even a 237-acre island. This larger coverage area carries with it more challenges, such as the necessity for more (or more powerful) sensors; interference from architectural features and competing radio sources; vulnerability of sensors to human adversaries; replacing batteries or sensors in hard-to-reach places; and modifying or augmenting the deployed sensors as new technology becomes available.

Static to mobile. An emerging area of research within the field of sensor networks focuses on using mobility to address the challenges associated with urban sensing. These *mobile sensor networks* differ from static sensor networks in many ways, and as we investigate the security of such systems, we have made some assumptions related to these differences.

Our initial assumption is that sensors are mobile and "people-centric"; that is, sensing not only the surrounding environment, but also people themselves. These sensors will be carried by people, either directly or in their vehicles, and therefore are conceptually tied to specific individuals. We envision sensors being built into devices such as cell phones, which are more powerful than traditional "mote" sensors and can be conveniently recharged on a daily basis, thus mitigating the extreme compute and energy constraints. We assume (for now) participation under a single administrative domain, and support from a public key infrastructure (PKI) or similar system to assert identity and attributes. Network availability and bandwidth—Wi-Fi and cellular—is much better in an urban environment than in the middle of a forest. Applications enabled by these systems will be directly and immediately relevant to users, and we assume that they will be willing to participate in such large-scale applications, adopting opportunistic practices for sensing and networking, for instance allowing their sensors to be remotely tasked on someone else's behalf. But we also make a few non-assumptions. Namely, we do not assume that the network infrastructure can be trusted, nor do we assume that sensors are tamper-proof or that users will not attempt to hack them. Similarly, we do not assume that sensors are always available, or never fail.

People-centric urban sensing has already been a topic of study in the community. We next overview two specific research projects along this direction, often used as points of reference in our exposition.

CarTel. The CarTel project [29] uses small Linux-based computers installed in vehicles to map traffic patterns in Boston and Seattle. The computer contains sensors of its own (e.g., GPS) and attaches to the vehicle's on-board diagnostic (OBD) interface to measure location, direction, speed, acceleration, and other relevant parameters. CarTel's delay-tolerant networking stack, CafNet, takes advantage of randomly-encountered unrestricted wireless access points to upload sensed data to a relational database on the Internet. A web-based user interface provides access to the database, and allows for modification of data-gathering

rules, such as time granularity. Applications enabled by the CarTel project include traffic monitoring, automotive diagnostics and notification, and road-surface diagnostics. Note that these applications are people-centric: the producers of the data are ordinary people (in their cars), and the consumers of this data are also ordinary users, not specialized scientists studying the environment.

MetroSense. Similarly, MetroSense [6] envisions a future in which the Internet is dominated by data from sensors carried by people around the world. The architecture is divided into three tiers: servers, sensor access points (SAPs), and the sensors themselves. Servers possess effectively unbounded storage and computing power, and are responsible for managing a MetroSense domain, including tasking of sensor devices, storing data, and running applications. The SAPs provide a gateway between sensors and servers, in addition to sensing their own environment and disseminating tasks to sensor nodes. The sensor tier consists of mobile sensors (MS) and static sensors (SS), both of which participate in the sensing of the world, and of the sensor's custodian. Some applications include BikeNet [17] and SkiScape [16], intended as sample studies to motivate the development of the MetroSense infrastructure.

Security in the mobile paradigm. As the sensor network field widens to include mobility in an urban environment, new security challenges are appearing. Additionally, some requirements of traditional networks are less important in the mobile, urban context, thus opening up new potential solutions.

One interesting side-effect of the shift to mobile sensing is that multi-hop routing seems less necessary. Through their experiments, the CarTel project revealed the existence of more than enough open wireless access points to allow the uploading of data to an aggregation point on the Internet. While connectivity is generally good in an urban environment, the sensors are still not connected 100% of the time. This intermittent connectivity leads to *delay-tolerant sensing*, where sensed data may be cached for a time before it is uploaded to an aggregation point. Furthermore, the multi-hop structure of many traditional networks (such as the Macroscope in the Redwoods and the counter-sniper system) inspired the development of secure routing protocols, but in urban-sensing scenarios, the focus should be on securing the data rather than securing the route.

Another facet of these new systems is their *people-centric* nature. Instead of trees and birds, they are sensing people: where they are and where they are going, what they are doing and what they are seeing. While these new aspects conjure up images of an amazing array of applications, they also present significant security challenges. We are not aware of any proposed people-centric urban sensing systems that incorporate security at the foundation of their design. Systems that ignore security and privacy, or that attempt to achieve such through security by obscurity, are inadequate and are unlikely to succeed. It is for these reasons that we seek to lay the groundwork for security in sensor networks, specifically those that involve mobile, people-centric sensors, by describing what we consider fundamental challenges in the area.

Perhaps the most obvious concern is the security of the sensed data itself, especially in correlation to the owner of the device. For example, from CarTel data it is trivial to deduce

the location of a participant's home within a small radius. How can this information be protected? Additionally, is it possible to allow selected people to see personal data at high fidelity, but to present a less accurate view to less trusted viewers?

A second critical concern is the integrity of the sensed data. An application based on sensor data is useless if users cannot trust the accuracy or timeliness of the data it consumes. Is it possible to operate an open, cooperative network of human-carried sensor devices when some of the people, or some elements of the infrastructure, cannot be trusted to communicate sensor data accurately and quickly?

In some urban-sensing visions, individual sensor nodes are dynamically tasked by remote applications. Metrosense incorporates the idea of *opportunistic tasking* [6], in which a sensor is given a task to perform for another, based upon its sensing capabilities, apparent direction, and other attributes. In this context, a task could ask for particular sensor readings to be gathered by sensors fulfilling certain criteria. For example, an application measuring average temperature in a specific room could emit a task requesting temperature readings every five minutes from sensor nodes whose GPS units indicate they are within the room. Taking this further, nodes could inform a central authority of some of their state (e.g., location and available hardware sensors) to facilitate better planning of tasks.

Earlier research on "retasking" static sensor networks has netted secure solutions such as Deluge [15] and Sluice [35]. It is unclear, however, if these solutions are applicable under the mobile paradigm where sensors are owned and operated by many different parties. How can the sensor be sure that the incoming request is legitimate? Are such systems susceptible to denial of service attacks, and if so, how can they be mitigated? Could a user somehow control which third parties use her sensor for their purposes?

Another marked difference from traditional sensor networks is that urban networks are not a carefully deployed set of trusted sensors. Just as sensors cannot categorically trust incoming traffic, the data reported by a sensor may be unreliable because of damage or tampering, both of which are probably more likely in the people-centric setting. Therefore, how can the data returned by a tasked sensor be trusted? If we task personal devices to collect sensor data for others, this raises several security and privacy risks.

It is these questions that drive our investigation and elaboration into security challenges in mobile, people-centric urban sensor networks.

3 Applications

In this section we give a few examples of people-centric urban-sensing applications to motivate that paradigm and to motivate the accompanying security challenges.

Urban data collection and processing. We anticipate that the people-centric paradigm will encourage large-scale, on-line data collection and processing of context information related to aspects of every-day life. Such information describes not only the physical environment but also captures some aspects of the social behavior of the people living in this environment.

For instance, an Active Map represents the location and context of people on a geographical map. For example, students at a university can view the location of their friends on

campus, and possibly information collected by personal and embedded sensors (indicating, for example, that they are in a conversation or are asleep). PARCTAB [57] was one of the seminal projects that provided users with devices whose location could be tracked and used for enhanced communication, including an active map. More recently, companies such as Dodgeball[1] and Boost Mobile[2] have started providing location-based "friend finder" services, where users are notified of friends in the vicinity, or can view the locations of their friends on a map. Soon we expect that sensor information in addition to location will be shared via such services. Active Maps could also display historical information, such as a map of the most frequently used running trails, indicating which may be muddy or contain steep uphill sections. BikeNet [17] is one such project, aimed at cyclists who would like to share real-time sensor data.[3] The map can also be an interface for registering context-sensitive triggers, such as "remind me to buy milk when I am next driving past the grocery store" or "alert me when both Bob and Alice are back in the office," or "let me know when a tennis court is available at the park."

Environmental monitoring at the human level. With human-centric sensing, applications that monitor the human environment (such as building maintenance, emergency rescue, ventilation and heating) now may become more efficient and useful. It becomes possible to sense and collect information (such as indoor air temperature) at the human level. Thus, the environment is sensed exactly where its semantics are important: at the human, rather than on the wall. One could optimize energy usage, for example, by reducing effort to heat, cool, or ventilate classrooms when the classroom appears empty, or to adjust office temperature as needed for the person sitting at the desk in the corner.

Indeed, if people carry devices that include environmental sensors, environmental monitoring can be achieved with far less static infrastructure. For example, people-centric devices can monitor the environment for hazardous gases, generating alerts or collecting long-term trends.

Towards sensing-based information systems. People-centric urban sensing may encourage on-line, context-aware information systems that inform, educate or entertain. Imagine a context-aware publish-subscribe system; sensor information is "tagged" with attributes as it is published into the system, and users subscribe to information based on tags of interest to them. Some tags are inherent to the sensor type, or the context (location, time) of the reading, and others may be applied by the carrier (much as tags are used on the web today). For example, a biker may subscribe to information about bike trails and traffic congestion; an allergy sufferer may subscribe to pollen-count sensors; a film-lover may subscribe to information about the length of lines at theaters.

Discussion. Admittedly, urban sensing covers a wide range of target applications and involves various new data dissemination components. At the core of this new setting is the ability to sense and process the large volumes of data sensed in complex urban environments.

[1] http://www.dodgeball.com

[2] http://www.boostmobile.com

[3] Also see http://metrosense.cs.dartmouth.edu/metro-projects.html

Accordingly, our study focuses on security challenges that are related to the sensing aspect of the new second-generation sensor-networking capabilities. We next focus on the important security challenges related to *privacy*, *integrity* and *availability*: addressing privacy will allow concerned users to participate in sensing applications; providing integrity assurances will improve the trustworthiness of sensed data; improving the availability of sensed data will make opportunistic sensing more dependable.

4 Security Challenges

It should be clear that these applications raise serious security and privacy risks. An unrestricted dissemination of users' sensor data results in breaches of *privacy*; users will want to control the dissemination of information about themselves. Furthermore, since data originates from sensors that are under the control of other people, the *integrity* of the data comes under question. For example, a user may tamper with a sensor device to cause it to report false data, or misrepresent the location or time the data was sensed. Furthermore, the *availability* of the infrastructure is critical for these applications to remain useful. In this section we outline specific challenges regarding privacy, integrity, and availability.

4.1 Confidentiality and Privacy Issues

The confidentiality of sensor data goes far beyond the provision of a secure channel from the sensor node to some gateway node. Such encryption, and in particular key distribution, has already been well discussed in the sensor-network security literature.

Challenge 1: Context privacy

While several systems have been proposed to address location privacy [20, 26], usable mechanisms for context privacy have been lacking. It will be cumbersome for users to specify fine-grained policies (as has been suggested for location privacy) for several types of context—who should know whether they are awake, who should know whether they are in a conversation, who should get access to heart-rate information, and so on. In a people-centric urban sensing environment, context privacy is of high importance. As a first attempt, we have proposed *virtual walls* [32] as a usable metaphor for controlling access to users' context information. Virtual walls behave in a way that intuitively maps to real walls in the physical world. For example, *transparent* virtual walls allow the release of personal context information much as a person's physical actions are fully visible through a real transparent wall. We also define intuitive semantics for *translucent* and *opaque* virtual walls. Still, for a real-world deployment, several challenges remain: users may want more precise access control for some types of context information, and hybrid mechanisms are needed that can balance the ease of use and a larger degree of control. There are several instances where groups of users should take ownership over data—for example, a group of athletes may want to control access to their sensor information as a group. Negotiation of group policies in a seamless and usable way will be a challenge. Furthermore, it is desirable to have the negotiation preserve the privacy of users within the group, who may want to vote on policies without being implicated or

singled out. Lastly, an adversary may be able to infer restricted context information from other available context information. Care must be taken, therefore, to ensure that context is not leaked inadvertently.

We anticipate that *secure multiparty computation (SMC)* [22, 62] may be helpful; in SMC, functions can be evaluated while maintaining the privacy of the individual inputs. We also recommend exploring the use of trusted hardware for performance reasons. For example, a trusted server can receive all the users' inputs and compute the outcome within the aegis of the tamper-resistant trusted hardware [50, 52].

Challenge 2: Anonymous tasking

One of the exciting aspects of the new urban-sensing paradigm is that user devices may be opportunistically tasked to sense areas beyond the reach of the system's infrastructure. Tasking of users, however, can be a threat to their privacy. For example, assigning the task "measure temperature at location X" to Alice, will eventually reveal the time at which Alice visited location X. Furthermore, Alice may not want the system to know her location at the instant when she was tasked. It is important, therefore, to ensure that users can be tasked anonymously. In many cases, *what* is tasked is more important than *who* was tasked.

Delivering tasks to anonymous users may seem easy. For example, users can choose to not identify themselves with the system, and receive tasks through beacons. Users that wish to accept the tasks can notify the system (without revealing their identity) of their acceptance, and then finally report the data. Such an approach, however, does not give the system any guarantee that the user is likely to deliver on that task. It would be useful if the system could predict which users are most likely to visit a particular location and opportunistically task those devices specifically. Or perhaps, the system may want to task certain "reliable" classes of people for a particular task (we call this "attribute-based" tasking). Such functionality is at odds with anonymous tasking, and an approach that balances anonymity with location-prediction algorithms and attribute-based tasking is needed.

One solution that looks promising is to use attribute-based authentication. Several cryptographic primitives exist that allow users to prove that they possess a certain set of credentials without revealing their identity [9, 36, 45, 54]. Following such authentication, users can be given specific tasks as long as they possess the requisite attributes. Such techniques will interfere with approaches that rely on the users' identities for ensuring the integrity of sensed data. Solutions that address privacy, therefore, will need to be designed with data integrity in mind. We discuss challenges for integrity in Section 4.2.

Another solution would to be allow the system to task specific users (i.e., knowing their identities), without knowing their current location. This provides users with location privacy, and not necessarily anonymity (identity privacy) [2, 24]. For example, the system may want to task Alice, specifically, to sense a given location X. A mechanism to deliver tasks to Alice, whose present location is hidden, could rely on an anonymizing network [2, 12, 48].

It would also be interesting to address the privacy of the querier, i.e., the person issuing the tasks. Perhaps users will be willing to accept tasks from only certain users. This brings up the question of what level of privacy should be supported for queriers. Perhaps techniques from trust negotiation can be used [58, 59], in which both the querier and the user being tasked have their own requirements of each other. Some trust negotiation techniques such

as "hidden credentials" [4, 19, 33] address the privacy of users in trust negotiation.

Challenge 3: Anonymous data reporting

Regardless of whether tasks were delivered anonymously, users may want to report sensor data without the system knowing their current location. For example, Alice may want to report her personal sensor data to a trusted database, without the system knowing where she is at the time she uploads the data. Protecting Alice's location from the system infrastructure, however, can be challenging—simply identifying the wireless access point through which she makes a network connection can localize Alice.

As mentioned earlier, one solution is to use an anonymizing network to hide Alice's location while she is reporting data, e.g., by bouncing data from access-point to access-point several times before the data goes to the database. If one organization manages all the access points, however, a system administrator may be able to correlate routing information and infer Alice's location. Trusted-computing hardware platforms [50, 52] may solve this problem by ensuring that even the human operators of access points do not have access to sensitive routing information.

If Alice is concerned about the privacy of her location at the time she *collected* the sensed data, she could "fuzz" the location and time of the sensed information—to add some random jitter, within acceptable limits. Such perturbations may make it difficult to correlate or aggregate sensor information, however, unless the amount of error can be constrained. It may be possible to use techniques developed for privacy-sensitive data-mining and database queries [13, 55].

We discuss sensor-data aggregation in the following section, but briefly mention here that due to higher connectivity (e.g., Wi-Fi enabled sensor nodes), and more energy and bandwidth, the focus in people-centric urban sensing shifts away from in-network aggregation and towards back-end processing of sensor data.

Another interesting problem is that of status reporting. Users in the system may be interested in querying the *status* of various sensors in the network, and then make tasking decisions based on the characteristics of available sensors. Responses to status queries, however, can reveal enough information about the sensors' carriers to threaten their privacy. Such functionality appears to be at odds with anonymous tasking, and perhaps a standard set of information can be reported to the system, e.g., location and availability of (the anonymous) nodes.

4.2 Integrity Issues

If the system protects the privacy of the tasked nodes, using anonymizing techniques for example, how do we know when to believe the sensor data? We discuss integrity challenges next.

Challenge 4: Reliable data readings

Traditional sensor networks face the problem of data reliability; the literature already notes limitations on detecting or correcting data-pollution attacks [47, 56, 61]. In people-centric

environments, however, trustworthiness of data becomes more crucial: the adversary is no longer only a malicious outsider capturing a subset of sensor nodes; now any participant with an appropriately-configured device can report falsified data. Because users are in control of their own devices, they can more easily launch such an attack. Furthermore, given the more personal nature of applications, they have an increased interest in doing so. For instance, privacy issues or activities that expose anomalous behavior can now be considered strong incentives for people to perform simple data-pollution attacks to protect themselves. How could a system detect and correct such behaviors?

One promising solution area is redundancy. In a large-scale urban-sensing infrastructure, it may be possible to provide multiple sensor nodes with the same task. The system could then use appropriate statistical processing algorithms to estimate the validity of the data, or to remove polluted subsets. For instance, appropriate statistical mechanisms could detect bias or correct malicious responses in survey data. Moreover, since incorrect data can be introduced not only due to malicious user actions but also due to erroneous configurations of the sensor devices, additional correction mechanisms can be considered. These mechanisms can include the design of a dynamic process that monitors the sensing reliability of the sensor nodes. The process can maintain various confidence levels about the quality of sensors as well as adjust their sensing abilities. For instance, it can re-calibrate sensors with low confidence levels or even temporarily revoke the sensed data.

Another approach, based on game-theoretic principles, is to couple strong pollution-detection capabilities with punishment strategies (such as exclusion of misbehaving parties [1, 38]). If applied selectively, this approach could encourage fairness and provide a strong disincentive for misbehavior. Alternatively, a reputation-based algorithm could be used as incentive for cooperation by assigning more weight to data returned by trustworthy sensors, perhaps determined by consensus. Finally, certain ground-truth enforcing techniques can be used to increase the confidence level of sensed data measurements. For instance, if the system infrastructure includes some physically secure access points with sensors of their own (as proposed in Metrosense [6]), one can use these measurements as representative high-weight or "ground-truth" data points that help in detecting and correcting falsification attacks.

Challenge 5: Data authenticity

Another fundamental security problem is data authentication; that is, how can sensed data be delivered to a database or application with assurance that no intermediate devices have tampered with it? Furthermore, in applications that care about the identity of the user carrying the sensor (for example, to report Alice's location on an active map), how can the system ensure the identity of the sensor node and its custodian?

A significant amount of research has been conducted on data authenticity in static sensor networks, especially in the context of secure in-network data aggregation. Different threat models have been studied, including fault-tolerant computation of aggregates [10, 25, 41, 43] and secure aggregation in the presence of single [27, 31] or multiple [8, 47] adversarial sensor nodes. Also, different models of in-network data aggregation have been considered, including the star-based aggregation model [14, 39, 47] and the tree-based aggregation model [8, 61]. Aggregation of encrypted data is studied in [5, 7, 21].

Unfortunately, these solutions are not feasible for mobile sensor networks. First, previous authentication techniques assume the availability of a stable topological tree that spans the network's sensors. In a highly dynamic and mobile network no such tree structure exists or can be maintained. At the same time, opportunistic networking, opportunistic tasking, data muling, and delayed reporting create an inherently complex communication environment in which few assumptions can be made about node integrity. Moreover, the previous research using mobile sensor nodes has focused on sensors attached to animals and vehicles. Human carriers, however, introduce new challenges for maintaining node integrity. Namely, to authenticate a sensor node, and possibly the user carrying it, we need mechanisms to verify identity, group memberships, and other attributes. These factors would likely affect their access privileges and participation in protocols. Finally, this problem is made even more challenging by the conflict between user authentication to verify data and any potential desired anonymity of said data.

Thus we need new schemes to authenticate the user and her sensor device, and to ensure the integrity of the data, based on few assumptions about network topology. We have some advantages relative to existing sensor-network literature; we may assume that sensor nodes are fairly capable platforms, and that they frequently come into direct contact with network access points. Desired properties include computational- and bandwidth-efficient authentication, topology-independent techniques, resilience against malicious subsets of nodes and resistance against denial-of-service attacks. Results on the authentication of streams in arbitrary adversarial networks using cryptographically-enhanced error-correcting techniques [37, 42] may give some insight in this direction.

Challenge 6: System integrity

Another important aspect of integrity relates to the functionality of the underlying system. In principle, any operation (in addition to data collection) performed in a mobile, opportunistic, and highly untrusted sensor network will need some form of correctness verification.

For instance, these people-centric sensor networks, likely based on pervasive devices such as cell phones, are an application platform as well as a sensing device. These applications need to be able to authenticate the information they receive from the system, and to determine when to trust the tasks they are asked to perform. One possible solution is to develop task-specification languages that allow a node to verify that execution of a particular task will not compromise the node itself. Such a procedure presents a trade-off between simplicity of verification and flexibility in describing complex tasks. A long history of research on the safe execution of mobile code [53] should be instructive.

Also, information centers (e.g., the server tier in MetroSense [6]) will need to validate the integrity of actions (e.g., tasking, muling, data collection) performed by mobile nodes at remote sites, often in a delay-tolerant fashion. How, for instance, can the system administrator of a sensing-based information system be sure that tasking is executed correctly or that reported data not only is authentic but also temporally relevant? Suggested solutions on this front include developing efficient verification protocols that ensure secure data management and guarantee system integrity. Conceptually, the system administrator could maintain some secure cryptographic state of the entire system configuration, consisting of various topological, temporal, and user-related parameters. This cryptographic state could

be updated and used for verification as involved network nodes execute queries, tasking commands, and other operations. This general approach recalls early results on memory consistency checking [3].

In general, any mechanism designed for system integrity depends on the specific threat or trust model. For instance, in an application where the focus lies on collection and off-line fusion of sensed data, certain components of infrastructure may be considered trusted by the system administrator—e.g., SAPs in MetroSense [6] may be considered to have higher levels of trust, through either physical protection or the use of secure hardware.

4.3 Availability

Researchers have addressed some of the denial of service (DoS) issues for static sensor networks—for example, adversaries may gain control of sensors and try to flood the network or subvert the routing protocols to affect the network's reporting capabilities [60]. People-centric urban sensing, however, introduces different DoS issues because devices are already in the hands of potential adversaries. On the other hand, because we assume high connectivity (sensors are frequently in contact with a Wi-Fi or cellular access point, and thus multi-hop communications may rarely be needed), the sensor network itself is less susceptible (though not entirely immune) to DoS than in some sensor-network scenarios.

Challenge 7: Preventing data suppression

In these people-centric urban sensor networks, DoS attacks that limit the availability of data becomes one of the central concerns. Since users get tasked opportunistically, these users may configure their device to refuse to accept certain tasks, or accept but then ignore the tasks. (Contrast this behavior with "traditional" sensor networks, where installed sensors faithfully report data unless compromised by an external adversary.) Data-consuming applications are left at the mercy, and whims, of the individual participants. This problem is exacerbated by privacy concerns—if users feel unable to control access to their data, they will be loathe to carry the device, or permit tasks that report such sensor data. This effect reinforces the importance of the privacy challenges above.

Challenge 8: Participation

Unlike static sensor networks, where sensors are embedded in the infrastructure, people-centric urban sensing relies on the sensor devices carried by users. One of the major challenges today is to create incentives for users to carry such devices, especially if bulky or a threat to their privacy. The best approach is to incorporate the sensors into a device they want to carry (such as a cell phone or music player), and provide incentives that are compatible with users' needs and interests. If the device has applications with clear direct and indirect benefits for the user, has usable, strong measures that protect privacy, and is easy to carry, people will use it.

Challenge 9: Fairness

Many people-centric sensor applications provide direct benefits to the users who carry the sensor nodes. Thus, people have an incentive to cheat, to obtain better service for themselves than they fairly deserve. For example, users may cause the applications to task many other sensors to collect information for their own needs, without being willing to take on tasks for other users. Research on incentive-compatible peer-to-peer systems may provide useful insight here [18, 23].

5 Summary

In this paper we recognize the current interest in people-centric urban-sensing applications and infrastructure. Such applications have clear and substantial security and privacy challenges, which must be resolved if these systems have any hope of realizing their potential. We described 9 challenges, and offered conceptual solution approaches for each one.

Challenge 1: Context privacy
Challenge 2: Anonymous tasking
Challenge 3: Anonymous data reporting
Challenge 4: Reliable data readings
Challenge 5: Data authenticity
Challenge 6: System integrity
Challenge 7: Preventing data suppression
Challenge 8: Participation
Challenge 9: Fairness

We hope that this paper will create a substantive discussion around these challenges and encourage all researchers involved with urban-sensing and people-centric sensor networks to address security and privacy at a fundamental level within their system and application design. The future of the paradigm depends on it.

Acknowledgments

We thank Vijay Bhuse, Andrew Campbell, George Cybenko, Shane Eisenman, and the rest of the Metrosense team at Dartmouth College for their helpful comments.

References

[1] I. Abraham, D. Dolev, R. Gonen, and J. Halpern. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation. In *Proceedings 25th ACM Symposium on Principles of Distributed Computing (PODC)*, 2006.

[2] J. Al-Muhtadi, R. H. Campbell, A. Kapadia, D. Mickunas, and S. Yi. Routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments.

In *Proceedings of The 22nd IEEE International Conference on Distributed Computing Systems (ICDCS)*, pages 74–83, 2002.

[3] M. Blum, W. Evans, P. Gemmell, S. Kannan, and M. Naor. Checking the correctness of memories. In *Proc. 32nd Symp. Foundations of Computer Science*, pages 90–99, San Juan, PR, Oct 1991. IEEE Computer Society.

[4] R. W. Bradshaw, J. E. Holt, and K. E. Seamons. Concealing complex policies with hidden credentials. In *Eleventh ACM Conference on Computer and Communications Security, Washington, DC*, pages 146–157, Oct. 2004.

[5] H. Cam, S. Ozdemir, P. Nair, D. Muthuavinashiappan, and H. O. Sanli. Energy-efficient secure pattern based data aggregation for wireless sensor networks. *Computer Communications*, pages 446–455, Feb. 2006.

[6] A. Campbell, S. Eisenman, N. Lane, E. Miluzzo, and R. Peterson. People-centric urban sensing. In *The Second Annual International Wireless Internet Conference (WICON)*, pages 2–5. IEEE Computer Society Press, August 2006.

[7] C. Castelluccia and G. T. E. Mykletun. Synopsis diffusion for robust aggregation in sensor networks. In *Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, (MobiQuitous 2005)*, pages 109–117, 2005.

[8] H. Chan, A. Perrig, and D. Song. Secure hierarchical in-network aggregation in sensor networks. In *CCS '06: Proceedings of the 13th ACM conference on Computer and communications security*, pages 278–287, New York, NY, USA, 2006. ACM Press.

[9] D. Chaum and J.-H. Evertse. A secure privacy preserving protocol for transmitting personal information between organizations. In *CRYPTO*, 1986.

[10] J.-Y. Chen, G. Pandurangan, and D. Xu. Robust computation of aggregates in wireless sensor networks: distributed randomized algorithms and analysis. In *IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks*, page 46, Piscataway, NJ, USA, 2005. IEEE Press.

[11] J. Deng, R. Han, and S. Mishra. A performance evaluation of intrusion-tolerant routing in wireless sensor networks. In *2nd International Workshop on Information Processing in Sensor Networks (IPSN)*, Apr. 2003.

[12] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In *Usenix Security Symposium*, pages 303–320, Aug. 2004.

[13] I. Dinur and K. Nissim. Revealing information while preserving privacy. In *PODS '03: Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pages 202–210, New York, NY, USA, 2003. ACM Press.

[14] W. Du, J. Deng, Y. S. Han, and P. Varshney. A witness-based approach for data fusion assurance in wireless sensor networks. In *Proceedings of IEEE 2003 Global Communications Conference (GLOBECOM)*, 2003.

[15] P. K. Dutta, J. W. Hui, D. C. Chu, and D. E. Culler. Securing the deluge network programming system. In *IPSN '06: Proceedings of the fifth international conference on Information processing in sensor networks*, pages 326–333, New York, NY, USA, 2006. ACM Press.

[16] S. B. Eisenman and A. T. Campbell. Skiscape sensing. In *SenSys '06: Proceedings of the 4th international conference on Embedded networked sensor systems*, pages 401–402, New York, NY, USA, 2006. ACM Press.

[17] S. B. Eisenman, N. D. Lane, E. Miluzzo, R. A. Peterson, G.-S. Ahn, and A. T. Campbell. BikeNet: An opportunistic sensing system for cyclist experience mapping. Submitted to Mobisys '07, December 2006.

[18] M. Feldman and J. Chuang. Overcoming free-riding behavior in peer-to-peer systems. *SIGecom Exch.*, 5(4):41–50, 2005.

[19] K. Frikken, J. Li, and M. Atallah. Trust negotiation with hidden credentials, hidden policies, and policy cycles. In *13th Annual Network and Distributed System Security Symposium*, pages 157–172, Feb. 2006.

[20] B. Gedik and L. Liu. Location privacy in mobile systems: A personalized anonymization model. In *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, pages 620–629, Columbus, OH, USA, June 2005.

[21] J. Girao, D. Westhoff, and M. Schneider. Synopsis diffusion for robust aggregation in sensor networks. In *Proceedings of IEEE International Conference on Communications*, pages 3044–3049, 2005.

[22] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game or a completeness theorem for protocols with honest majority. In *STOC*, pages 218–229, 1987.

[23] P. Golle, K. Leyton-Brown, and I. Mironov. Incentives for sharing in peer-to-peer networks. In *Proc. of the 2001 ACM Conference on Electronic Commerce*, 2001.

[24] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless lan through disposable interface identifiers. *ACM Mobile Networks and Applications (MONET)*, 10:315–325, 2005.

[25] I. Gupta, R. van Renesse, and K. P. Birman. Scalable fault-tolerant aggregation in large process groups. In *DSN '01: Proceedings of the 2001 International Conference on Dependable Systems and Networks (formerly: FTCS)*, pages 433–442, Washington, DC, USA, 2001. IEEE Computer Society.

[26] B. Hoh and M. Gruteser. Protecting location privacy through path confusion. In *Proceedings of the IEEE/CreateNet Intl. Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, Athens, Greece, Sept. 2005.

[27] L. Hu and D. Evans. Secure aggregation for wireless networks. In *Proceedings of Workshop on Security and Assurance in Ad hoc Networks*, January 2003.

[28] D. Huang, M. Mehta, D. Medhi, and L. Harn. Location-aware key management scheme for wireless sensor networks. In *Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 29–42, Washington, DC, Oct. 2004.

[29] B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. K. Miu, E. Shih, H. Balakrishnan, and S. Madden. CarTel: A Distributed Mobile Sensor Computing System. In *4th ACM SenSys*, Boulder, CO, November 2006.

[30] J. Hwang and Y. Kim. Revisiting random key pre-distribution schemes for wireless sensor networks. In *Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 43–52, Washington, DC, Oct. 2004.

[31] P. Jadia and A. Mathuria. Efficient secure aggregation in sensor networks. In *Proceedings of High Performance Computing - HiPC 2004*, pages 40–49, 2005.

[32] A. Kapadia, T. Henderson, J. Fielding, and D. Kotz. Virtual walls: Protecting digital privacy in pervasive environments. In *Proceedings of the Fifth International Conference on Pervasive Computing (Pervasive)*, Lecture Notes in Computer Science. Springer-Verlag, May 2007. Accepted for publication; available at `http://www.cs.dartmouth.edu/~dfk/papers/kapadia:walls.pdf`.

[33] A. Kapadia, P. P. Tsang, and S. W. Smith. Attribute-based publishing with hidden credentials and hidden policies. In *The 14th Annual Network and Distributed System Security Symposium (NDSS '07) (To Appear)*, Mar. 2007.

[34] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In *Proc. of the First IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127. IEEE C. S. Press, May 2003.

[35] P. E. Lanigan, R. Gandhi, and P. Narasimhan. Sluice: Secure dissemination of code updates in sensor networks. In *ICDCS '06: Proceedings of the 26th IEEE International Conference on Distributed Computing Systems*, page 53, Washington, DC, USA, 2006. IEEE Computer Society.

[36] A. Lysyanskaya, R. Rivest, A. Sahai, and S. Wolf. Pseudonym systems. In *Selected Areas of Cryptography, Volume 1758 LNCS*, 1999.

[37] A. Lysyanskaya, R. Tamassia, and N. Triandopoulos. Multicast authentication in fully adversarial networks. In *Proceedings of IEEE Symposium on Security and Privacy (SSP)*, pages 241–255, May 2004.

[38] A. Lysyanskaya and N. Triandopoulos. Rationality and adversarial behavior in multi-party computation. In *Proceedings of Advances in Cryptology — CRYPTO '06*, pages 180–197, 2006.

[39] A. Mahimkar and T. S. Rappaport. Securedav: a secure data aggregation and verification protocol for sensor networks. In *Proceedings of Global Telecommunications Conference (GLOBECOM '04)*, pages 2175–2179, 2004.

[40] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson. Wireless sensor networks for habitat monitoring. In *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 88–97, New York, NY, USA, 2002. ACM Press.

[41] A. Manjhi, S. Nath, and P. B. Gibbons. Tributaries and deltas: efficient and robust aggregation in sensor network streams. In *SIGMOD '05: Proceedings of the 2005 ACM SIGMOD international conference on Management of data*, pages 287–298, New York, NY, USA, 2005. ACM Press.

[42] S. Micali, C. Peikert, M. Sudan, and D. A. Wilson. Optimal error correction against computationally bounded noise. In *Proceedings of 2nd Theory of Cryptography Conference (TCC)*, pages 1–16, 2005.

[43] S. Nath, P. B. Gibbons, S. Seshan, and Z. R. Anderson. Synopsis diffusion for robust aggregation in sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 250–262, New York, NY, USA, 2004. ACM Press.

[44] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler. SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, Sept. 2002.

[45] P. Persiano and I. Visconti. An Anonymous Credential System and a Privacy-Aware PKI. In *R. Safavi-Naini and J. Seberry, editors, Information Security and Privacy, 8th Australasian Conference, ACISP 2003, volume 2727 of Lecture Notes in Computer Science. Springer Verlag*, 2003.

[46] K. Piotrowski, P. Langendoerfer, and S. Peter. How public key cryptography influences wireless sensor node lifetime. In *SASN '06: Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, pages 169–176, New York, NY, USA, 2006. ACM Press.

[47] B. Przydatek, D. Song, and A. Perrig. SIA: Secure information aggregation in sensor networks. In *SenSys '03: Proceedings of the 1th international conference on embedded networked sensor systems*, New York, NY, USA, 2003. ACM Press.

[48] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for Web Transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, Nov. 1998.

[49] G. Simon, M. Maróti, Ákos Lédeczi, G. Balogh, B. Kusy, A. Nádas, G. Pap, J. Sallai, and K. Frampton. Sensor network-based countersniper system. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 1–12, New York, NY, USA, 2004. ACM Press.

[50] S. W. Smith and S. Weingart. Building a high-performance, programmable secure coprocessor. *Computer Networks (Special Issue on Computer Network Security.)*, 31:831–860, Apr. 1999.

[51] G. Tolle, J. Polastre, R. Szewczyk, D. E. Culler, N. Turner, K. Tu, S. Burgess, T. Dawson, P. Buonadonna, D. Gay, and W. Hong. A macroscope in the redwoods. In *SenSys*, pages 51–63, 2005.

[52] Trusted computing group, May 2005. `https://www.trustedcomputinggroup.org/home`.

[53] C. F. Tschudin. Mobile agent security. In M. Klusch, editor, *Intelligent Information Agents*, chapter 18, pages 431–445. Springer-Verlag, 1999.

[54] E. R. Verheul. Self-Blindable Credential Certificates from the Weil Pairing. In *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*, pages 533–551. Springer-Verlag, 2001.

[55] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, Y. Saygin, and Y. Theodoridis. State-of-the-art in privacy preserving data mining. *ACM SIGMOD Record*, 3(1):50–57, March 2004.

[56] D. Wagner. Resilient aggregation in sensor networks. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 78–87, New York, NY, USA, 2004. ACM Press.

[57] R. Want, B. Schilit, N. Adams, R. Gold, K. Petersen, J. Ellis, D. Goldberg, and M. Weiser. The PARCTAB ubiquitous computing experiment. Technical Report CSL-95-1, Xerox Palo Alto Research Center, Mar. 1995.

[58] W. H. Winsborough and N. Li. Towards practical automated trust negotiation. In *Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks*, pages 92–103, June 2002.

[59] W. H. Winsborough, K. E. Seamons, and V. E. Jones. Automated trust negotiation. In *DARPA Information Survivability Conference and Exposition (DISCEX)*, pages 88–102, Jan. 2000.

[60] A. D. Wood and J. Stankovic. Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62, 2002.

[61] Y. Yang, X. Wang, S. Zhu, and G. Cao. SDAP: a secure hop-by-hop data aggregation protocol for sensor networks. In *MobiHoc '06: Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing*, pages 356–367, New York, NY, USA, 2006. ACM Press.

[62] A. Yao. Protocols for secure computations. In I. C. Society, editor, *Proceedings of the twenty-third annual IEEE Symposium on Foundations of Computer Science*, pages 160–164, 1982.

[63] S. Yi and R. Kravets. Composite key management for ad hoc networks. In *The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004 (MOBIQUITOUS)*, pages 52–61, Aug. 2004.

[64] C. Yin, S. Huang, P. Su, and C. Gao. Secure routing for large-scale wireless sensor networks. In *Proc. of International Conference on Communication Technology (ICCT)*, Apr. 2003.

[65] S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for large-scale distributed sensor networks. In *Proc. of the 10th ACM conference on Computer and communications security (CCS)*, pages 62–72. ACM Press, 2003.