The Smart Citizen Factor in Trustworthy Smart City Crowdsensing

Maryam Pouryazdan and Burak Kantarci, *Clarkson University*

This article surveys the state of the art in reputation-based crowdsensing in smart cities. The authors also present a vote-based, reputation-aware user-recruitment approach that unveils the impact of collaborative trustworthiness assessment using anchor smart citizens.

Smart cities aim to improve quality of life by consolidating ICT infrastructure into physical and social infrastructure in urban environments.[1] This consolidated infrastructure offers citizens various services that are interconnected via ICT. Core smart services include administration, education, healthcare, public safety, transportation, and utilities. The smart city infrastructure consists of an application layer in which services are delivered to citizens; a network layer in which users, data sources, and service providers communicate; and a perception layer in which data acquisition and recruitment of sensing devices take place.[2]

The advent of the Internet of Things (IoT) paradigm in everyday life has empowered personal mobile devices, improved the perception layer in a smart city infrastructure, and affected the two upper layers. Wireless sensor networks, RFID tags, and built-in sensors in smartphones and wearable devices will help realize device-level connectivity in smart cities. Integrating IoT devices, cloud computing, and data analysis into the smart city architecture accelerates the improvement of smart city services.[3]

We can consider the basic building blocks of a smart city to be smart management of urban services, smart homes, smart energy, smart transportation, smart water, and smart citizens. The

 Published by the IEEE Computer Society

first five have been studied and stressed more than the final block—smart citizens. However, according to Ericsson's 2014 consumer insight summary report, smart citizens are major drivers of a smart city.[4] With the rise of IT in smart cities, smart citizens have been actively participating in the monitoring, interpreting, and decision-making processes in these applications. This gives rise to the following question: What makes a smart citizen? Basically, smart citizens are individuals using mobile smart devices (such as smartphones) who contribute to the collective monitoring of the city through those devices' sensing and processing capabilities. This concept is also known as *sensing as a service*.[5]

Here, we describe the benefits of the smart citizen factor in smart city crowdsensing, detect open issues and challenges, present a user-driven viable solution to improving the trustworthiness of crowdsensed data, and provide insights for paving the way toward effective mobile crowdsensing for smart cities.

Mobile Crowdsensing Benefits and Challenges

Mobile crowdsensing stems from the concept of participatory sensing, and involves mobile social networks and smart mobile devices through which data can be collected either explicitly or implicitly from users.[6] With implicit participation, users require effective incentives to grant access to their smartphones' built-in sensing resources. New business models are needed to recruit users whose primary interest is not the sensing task the crowdsensing platform requires.

Related work describes platform- and user-centric incentives for recruiting users who are mostly implicit participants.[7,8] Such users are rewarded based on the value of data received through the built-in sensors in their smartphones. Rewards do not have to be in cash—they can be additional data packages from the wireless operator, exclusive add-ons for wireless plans, special discounts on some services, and so on. Although truthfulness can be an issue—with greedy users aiming to increase their rewards—trustworthiness arises as a greater challenge because there is always a risk of adversaries spreading disinformation through the crowdsensing platform for various reasons. Reputation-based systems help address this issue,[9] such that recruitment of a particular user for an upcoming crowdsensing task is a function of a set of parameters that includes that user's reputation. This business model will offer benefits in three main areas.

The public benefits are two-fold: The value of the data that the crowdsensing platform provides is the most significant public benefit. In addition, as mobile device users are rewarded based on the usefulness of the data they provide, economic benefits become possible.

Business benefits pertain to businesses' ability to offer "X as a service" to end users; X might refer to analytics and visualization (that is, software), computing and storage resources (infrastructure), or cloud platforms for application developers in crowdsensing.

Finally, benefits to government arise because smart city applications are wide-ranging and include smart transportation, smart metering, and public safety, which require regulatory efforts from governmental administrative divisions. Because data will be provided by citizens and analyzed in a cloud platform, these divisions can reduce investment costs for infrastructure monitoring in smart cities and maintain powerful monitoring systems by purchasing analytics and visualization as a service from providers.

Benefits to government arise because smart city applications are wide-ranging and include smart transportation, smart metering, and public safety.

Ensuring Trustworthiness in Mobile Crowdsensing

Related work reports that the trustworthiness of a regular user and an adversary reveals the following behavioral difference in a mobile crowdsensing system. The system recruits users with high reputations with higher probability, whereas users with low reputations will be recruited with low probability, letting them continue to build reputation as long as they provide true sensor readings.[9] In one study, three types of reports are proposed to achieve trustworthiness goals in mobile crowdsensing:[10] S-reports, U-reports, and E-reports, denoting sensing activity reports, reports from review

requests, and reports by authorities, respectively. In that study, S-reports and U-reports are used to assess user credibility. Generally, reputation-aware works rely on S-report-like information to assess the trustworthiness of crowdsensed data.

As mentioned, multiple factors affect the recruitment process, and setting up effective incentives for implicit participants is of paramount importance. Therefore, trustworthiness assurance is tightly linked to the incentive mechanism that is used by the platform to recruit users. In prior work,[9] one of us (Burak Kantarci) proposed Trustworthy Sensing for Crowd Management (TSCM), which adopts the MSensing auction approach[7] and integrates it with statistical reputation awareness. Statistical reputation denotes the ratio of true sensor readings to total readings, whereby a false reading is identified through an outlier detection algorithm. Users join the auction by reporting their sensing costs, which are called *bids*, and are guaranteed to be rewarded no less than their bids.

Machine intelligence should be combined with human intelligence to meet complementary goals in mobile crowdsensing.

On the other hand, given that every sensing task has a value, the crowdsensing platform aims to maximize its total utility, which is the difference between the total value of sensed tasks and the total rewards made to participants. The value of a sensing task is scaled by the average reputation of the selected users. Given that malicious users are potentially bidding lower than their actual sensing costs—with the objective of being selected in the auction—the reported bids are also scaled by reputation value so that those with higher reputation are more likely to be selected, and more likely to be rewarded better if they are selected. Because location is a key parameter in participant selection, Mobility-Aware Trustworthy Crowdsensing (MATCS)[11] runs a trajectory estimation method by assuming that smartphone users follow the random waypoint mobility model, and recruits users based on their future location via MSensing auction. In Trustworthy-Mobile Social Network-Aware Crowdsensing (T-MSNAC), future locations were predicted based on their social attractiveness.[12]

Although statistical reputation works well under various scenarios, in large-scale crowdsensing, more scalable solutions might be needed in which reputation assessment is driven directly by participating smart citizens. Therefore, we next discuss distributed reputation-awareness and trustworthiness assurance in smart city crowdsensing.

Smart Citizens and Vote-Based Trustworthiness

Because mobile crowdsensing denotes large-scale user participation, decentralized solutions to obtain and maintain user reputation have emerged for the sake of scalability. Therefore, intelligence to detect adversaries can be decoupled from the crowdsensing platform, which should be responsible primarily for aggregating, analyzing, and visualizing crowdsensed data to end users.

As mentioned elsewhere,[13] machine intelligence should be combined with human intelligence to meet complementary goals in mobile crowdsensing. Among these goals, machine intelligence can provide data mining and knowledge discovery, as well as data quality assessment and assurance; it can be complemented by human intelligence through extended abilities such as cognition and decision making, as well as behaviors and contexts, including preferences and social interactions. Inspired by this argument, we endorse the active involvement of smart citizens in offloading the computational and storage burden on the crowdsensing platform to maintain a large distributed user reputation database. Furthermore, this idea has been proposed for smart cities.[14]

Vote-based trustworthiness assurance adopts the Sybil detection mechanism for social networks.[15] Basically, when a new user joins a community, his or her reputation is voted on by other users in the same community. Figure 1 illustrates a simple scenario of vote-based trustworthiness assurance in mobile crowdsensing.

As the figure illustrates, sensing the same phenomenon defines an interaction between two users—that is, the two users get connected. The mobile application for crowdsensing has access to all built-in sensors, and it can access all previous readings of a user's current connections.

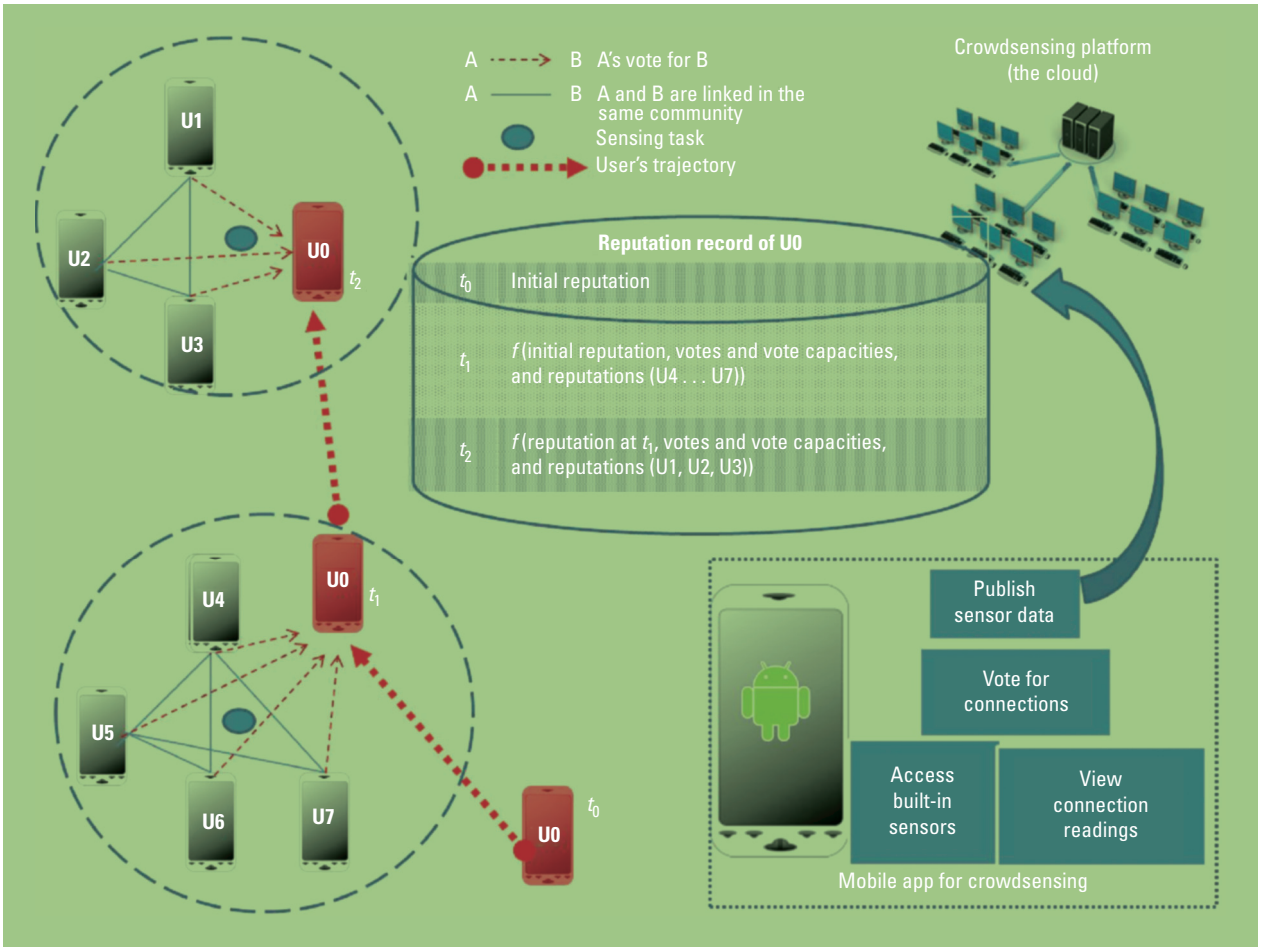

Figure 1. Smart citizen-driven vote-based trustworthiness assurance. A community consists of the users that have been assigned common sensing tasks during a recent time window. All members of a community vote on the reputation of a newly joining user.

Based on these access privileges, the mobile application publishes sensor readings, as well as its votes for the connections on the crowdsensing platform, which is hosted in the cloud. In the figure, at t_0, user 0 (U0) does not have any connections, but has an initial (or default) reputation assigned upon installing the application.

At t_1, U0 gets in range of a sensing task that is being sensed by four other users (U4–U7) who already had common sensing tasks. Besides their own vote, all users have a vote capacity and a reputation value. Upon sensing the task, every user votes for U0's reputation, and all votes are aggregated by a function that takes U0's previous reputation and a weighted sum of all votes, vote capacities, and reputations normalized by the total vote capacity of the voting members. U0 inherits the average vote capacity of its community members.

At t_2, U0 joins another community that consists of three other users (U1–U3) who run the same voting mechanism to update U0's reputation. It is worthwhile to mention that only the users who have been selected for crowdsensing are illustrated in this figure. Because the business model is built to maximize the utility of the crowdsensing platform (that is, the value of the data) and the utility of the participants (that is, the rewards), only a subset of users that show interest in a particular sensing task can be recruited. The selection process is based on an auction procedure in which the value of crowdsensed tasks is scaled by the average reputation of the recruited users, while a user's reward is also adjusted based on his or her reputation. Further details of the user recruitment process are available in prior work.[9]

Anchor Smart Citizens

Although relying on the votes of smart citizens can be beneficial for the crowdsensing system,

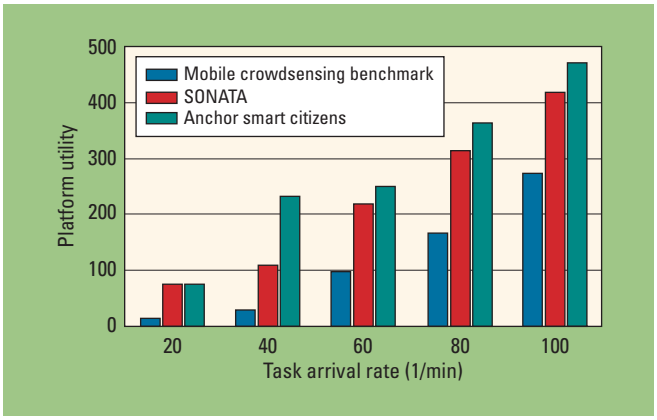

Figure 2. The impact of anchor smart citizens on platform utility. Having anchor citizens in the crowdsensing terrain leads to a platform utility improvement of up to 60 percent.

voter reliability could lead to a risky situation when malicious users collaborate to cast negative votes for reputable users and positive votes for malicious ones. To overcome this situation while maintaining the benefits of vote-based trustworthiness assurance in mobile crowdsensing, a hierarchical reputation model can be used in which some smart citizens act as trusted agents of the crowdsensing system. We call this group of users *anchor smart citizens* to denote their constant, 100 percent credibility and full vote capacity, whereas non-anchor citizens have dynamic vote capacities and reputations. Indeed, this approach is coherent with the E-reports-based credibility idea.[10] Thus, if the reputation management and trustworthiness assurance mechanism in Figure 1 is adopted by identifying a group of users as anchors, the reputation of the anchors will remain unchanged, whereas the anchors will increase the vote capacities and reputation of the users that they have voted for. Moreover, an anchor user

- might report false sensor data due to sensor malfunctioning, but this will not damage his or her reputation in a crowdsensing system;
- uses the same method as other users in the community when deciding to cast a positive or negative vote for a newly joining user—thus, an anchor does not have any additional capability to identify a malicious user;
- helps regular users build reputation in crowdsensing systems via his or her positive votes for them; and
- has to be rewarded just like a non-anchor user.

We have redesigned the smart citizens and vote-based trustworthiness approach and have identified a certain proportion of the crowdsensing population as anchors. Note that determining the anchor proportion is a grand design challenge in this system. Based on prior work,[9] we concluded that it is realistic to assume that no more than 5 percent of users are malicious. We have run extensive simulations to empirically determine the size of the anchor population. By setting the malicious users, as well as the anchor citizens, at 5 percent of the population, we simulated a crowdsensing system of 1,000 users uniformly deployed on a 1,000 × 1,000-unit terrain, where 30 units of range defines the sensing task interest for a smartphone.

Although the arrival rates of sensing task requests at random locations varied between 20 tasks/min and 100 tasks/min with Poisson distribution, initial reputations were set to 0.7 for regular users. The initial vote capacity of non-anchor users was set to a random value in (0,1]. The sensing costs (user bids) varied between 1 and 10, in which the value of a sensing task was randomly chosen from the set {1, 2, ..., 5}. Any user can detect the malicious behavior of its connections with a certain probability based on the connection's previous readings. Based on earlier work, we set this probability at 20 percent.[14] The initial vote capacity of non-anchor users was set to a random value in (0,1]. Similar to previous work,[14] a user's instantaneous and historical reputation have equal impact on his or her overall trustworthiness. The accuracy of a built-in sensor is assumed to be [0.97–0.98].[9] For the sake of simplicity, we do not consider the mobility of smartphone users.

Figure 2 compares the anchor smart citizen-driven vote-based approach to Social Network Assisted Trustworthiness Assurance (SONATA) and a benchmark of mobile crowdsensing that basically adopts MSensing auction. Smart citizen-driven vote-based trustworthiness assurance can enhance platform utility up to the order of 50 percent, whereas having anchor citizens in the crowdsensing terrain leads to a platform utility improvement of up to 60 percent.

Because users are recruited following an auction procedure, we might wonder how user utilities behave under the anchor smart citizen-driven approach. As seen in Figure 3a, the benchmark crowdsensing approach that adopts MSensing auction with no reputation-awareness introduces

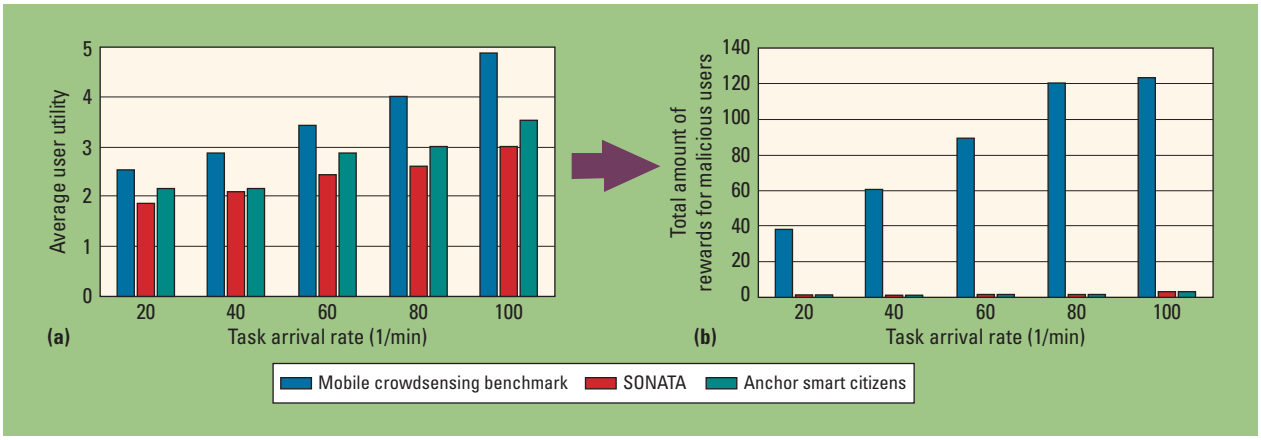

Figure 3. The impact of anchor smart citizens on user utility and payment to malicious users. (a) The benchmark crowdsensing approach introduces the highest user utility, and (b) vote-based approaches make negligible payments to malicious users.

Table 1. Summary and comparison of surveyed solutions.

Application	Platform utility	User utility	Reputation	User recruitment	Trustworthiness methodology
MSensing[7]	High	High	×	Auction/game	N/A
Trustworthy Sensing for Crowd Management [9]	High	Medium	√	Auction	Statistical
Mobility-Aware Trustworthy Crowdsensing [11]	High	Medium	√	Auction/mobility prediction	Statistical
Trustworthy-Mobile Social Network-Aware Crowdsensing [12]	High	Medium	√	Auction/social awareness	Statistical
Mobile Pervasive Accessibility Social Sensing (mPASS) [10]	High	N/A	√	Auction	Accessibility report-based
Social Network Assisted Trustworthiness Assurance (SONATA)[14]	High	Medium	√	Auction	Vote-based
Anchor smart citizens	High	High	√	Auction	Vote-based

the highest user utility. The reason for this can be explained when we look at Figure 3b, which presents payments to malicious users. As seen in this figure, vote-based approaches make negligible payments to malicious users. Furthermore, as seen in Figure 3a, having anchor users in the terrain increases the accuracy of the voting mechanism, and more users are rewarded based on the usefulness of their data, as well as their reputation.

Possible Application Areas

There are several ongoing applications in smart city crowdsensing, and trustworthiness is a priority issue in those fields. The smart citizen factor can help improve the trustworthiness of collected data in almost any crowdsensing application because mobile crowdsensing relies on sensor data reported by pseudonymous individuals.

A critical application is the roadside crowdsensing phenomena, which, through sensor data, reports acceleration, speed, and compass or multimedia data uploaded by a driver's camera.[16] In this scenario, trustworthiness arises as a crucial concern because city administration might be misled by malicious users through altered or fake sensor

data. Besides traffic conditions, road conditions can be monitored as introduced by the vCity Map application, in which vibration data is collected from participating cyclists.[17] Although trustworthiness is important in these applications, in scenarios where crowdsensing is used for disaster recovery, a lack of trustworthiness in the data could lead to more severe consequences.[18] Similarly, public safety applications can be elevated through crowdsensing because smartphones can also provide accelerometers, gyroscopes, and GPS data as a service to monitor crowd density and recognize human activities.

Besides these applications, smart water systems via mobile crowdsensing have not been studied well. Water monitoring requires biosensors, and it is possible to interface bio-sensors via portable sensors that can be attached to smartphones. Smart manufacturing is another application area in which environmental conditions can be crowdsensed with minimal investment.

Table 1 summarizes and compares the surveyed schemes in this article. Here, we considered anchor smart citizens, as well as other users, as fixed entities in the crowdsensing system. However, mobility-aware location prediction schemes should complement crowdsensing based on anchor smart citizens. Given that the success of the anchor-based approach is closely related to the ratio of anchor smart citizens, the social circles of such citizens should also be considered to predict their trajectories. Moreover, our current research is integrating vote-based trust scores into users' statistical reputations so that both the centralized and smart citizen-driven credibility of a user can be obtained. Furthermore, the incorporation of more advanced attack scenarios, such as mobile devices using adaptive thresholds to trigger or pause manipulation, is included in extensions to this study. We do not consider rotating the anchor role among smart citizens based on the battery level of their smartphones; hence, updating the set of anchor smart citizens remains an unaddressed research problem.

Last but not least, data collection in a challenging application such as smart water will introduce various reliability issues due to environmental factors or interference due to sensors' electrochemical properties. Identifying some nodes as anchors will help improve the value of crowdsensed data in these applications.

Acknowledgments

This material is based on work supported by the US National Science Foundation (NSF) under grant no. CNS1464273.

References

1. M. Naphade et al., "Smarter Cities and Their Innovation Challenges," *Computer*, vol. 44, no. 6, 2011, pp. 32–39.
2. K. Su, J. Li, and H. Fu, "Smart City and the Applications," *Proc. Int'l Conf. Electronics, Comm., and Control* (ICECC), 2011, pp. 1028–1031.
3. C.E.A. Mulligan and M. Olsson, "Architectural Implications of Smart City Business Models: An Evolutionary Perspective," *IEEE Comm.*, vol. 51, no. 6, 2013, pp. 80–85.
4. Ericsson ConsumerLab, *Smart Citizens: How the Internet Facilitates Smart Choices in City Life*, Nov. 2014, www.ericsson.com/res/docs/2014/consumerlab/ericsson-consumerlab-smart-citizens.pdf.
5. X. Sheng et al., "Sensing as a Service: Challenges, Solutions, and Future Directions," *IEEE Sensors J.*, vol. 13, no. 10, 2013, pp. 3733–3741.
6. B. Guo et al., "From Participatory Sensing to Mobile Crowd Sensing," *Proc. IEEE Int'l Conf. Pervasive Computing and Comm. Workshops* (PERCOM), 2014, pp. 593–598.
7. D. Yang et al., "Crowdsourcing to Smartphones: Incentive Mechanism Design for Mobile Phone Sensing," *Proc. 18th Int'l Conf. Mobile Computing and Networking* (Mobicom), 2012, pp. 173–184.
8. S. Huangfu et al., "Using the Model of Markets with Intermediaries as an Incentive Scheme for Opportunistic Social Networks," *Proc. IEEE 10th Int'l Conf. Ubiquitous Intelligence and Computing and 10th Int'l Conf. Autonomic and Trusted Computing* (UIC/ATC), 2013, pp. 142–149.
9. B. Kantarci and H.T. Mouftah, "Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things," *IEEE Internet of Things J.*, vol. 1, no. 4, 2014, pp. 360–368.
10. C. Prandi et al., "Trustworthiness in Crowd-Sensed and Sourced Georeferenced Data," *Proc. IEEE Int'l Conf. Pervasive Computing and Comm. Workshops* (PERCOM), 2015, pp. 402–407.
11. B. Kantarci and H.T. Mouftah, "Mobility-Aware Trustworthy Crowdsourcing in Cloud-Centric Internet of Things," *Proc. IEEE Int'l Symp. Computers and Communications* (ISCC), 2014; doi: 10.1109/ISCC.2014.6912581.

12. B. Kantarci and H.T. Mouftah, "Trustworthy Crowdsourcing via Mobile Social Networks," *Proc. IEEE Global Comm. Conf.* (GLOBECOM), 2014, pp. 2905–2910.
13. B. Guo et al., "Building Human-Machine Intelligence in Mobile Crowd Sensing," *IT Professional*, vol. 17, no. 3, 2015, pp. 46–52.
14. B. Kantarci, K.G. Carr, and C.D. Pearsall, "SONATA: Social Network Assisted Trustworthiness Assurance in Smart City Crowdsensing," *Int'l J. Distributed Systems and Technologies*, vol. 7, no. 1, 2016, pp. 64–84.
15. Z. Yang et al., "VoteTrust: Leveraging Friend Invitation Graph to Defend Against Social Network Sybils," *IEEE Trans. Dependable and Secure Computing*, 2015, pp. 1–14.
16. K. Aihara et al., "Crowdsourced Mobile Sensing for Smarter City Life," *Proc. IEEE 7th Int'l Conf. Service-Oriented Computing and Applications* (SOCA), 2014, pp. 334–337.
17. Y. Tobe et al., "vCity Map: Crowd-Sensing Towards Visible Cities," *Proc. IEEE SENSORS Conf.*, 2014, pp. 17–20.
18. S. Hu et al., "On Exploiting Logical Dependencies for Minimizing Additive Cost Metrics in Resource-Limited Crowdsensing," *Proc. Int'l Conf. Distributed Computing in Sensor Systems* (DCOSS), 2015, pp. 189–198.

Maryam Pouryazdan *is a PhD student in the Department of Electrical and Computer Engineering at Clarkson University, New York. Her research interests include trustworthiness assurance in crowdsensing via mobile social networks. Pouryazdan received an MSc in computer engineering from the University of Technology–Malaysia. She is a student member of IEEE. Contact her at pouryam@clarkson.edu.*

Burak Kantarci *is an assistant professor in the Department of Electrical and Computer Engineering at Clarkson University, New York. His research interests include Internet of Things, big data in the network, social networks, cloud networking, and digital health systems. Kantarci has coauthored more than a hundred papers in established journals and conferences, and contributed to 11 book chapters. He received a PhD in computer engineering from Istanbul Technical University, and is a senior member of IEEE. Contact him at bkantarc@clarkson.edu.*