Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things

Burak Kantarci, *Senior Member*, *IEEE*, and Hussein T. Mouftah, *Fellow*, *IEEE*

***Abstract*—The Internet of Things (IoT) paradigm stands for virtually interconnected objects that are identifiable and equipped with sensing, computing, and communication capabilities. Implementation of services and applications over the IoT architecture can take benefit of the cloud computing concept. Sensing-as-a-Service (S^2aaS) is a cloud-inspired service model which enables access to the IoT. In this paper, we present a framework where IoT can enhance public safety by crowd management via sensing services that are provided by smart phones equipped with various types of sensors. In order to ensure trustworthiness in the presented framework, we propose a reputation-based S^2aaS scheme, namely, Trustworthy Sensing for Crowd Management (TSCM) for front-end access to the IoT. TSCM collects sensing data based on a cloud model and an auction procedure which selects mobile devices for particular sensing tasks and determines the payments to the users of the mobile devices that provide data. Performance evaluation of TSCM shows that the impact of malicious users in the crowdsourced data can be degraded by 75% while trustworthiness of a malicious user converges to a value below 40% following few auctions. Moreover, we show that TSCM can enhance the utility of the public safety authority up to 85%.**

***Index Terms*—Auction theory, cloud computing, crowd management, Internet of Things (IoT), public safety, Sensing-as-a-Service (S^2aaS), smart phone sensing, social networking.**

I. Introduction

THE Internet of Things (IoT) paradigm denotes the pervasive and ubiquitous interconnection of billions of embedded devices that can be uniquely identified, localized, and communicated [1]. IoT architecture can be implemented as either Internet centric or object centric. The former aims at provisioning services within the Internet, where data are contributed by the objects whereas the latter aims at provisioning services via network of smart objects. Scalability and cost-efficiency of IoT services can be achieved by the integration of cloud-computing into the IoT architecture, i.e., cloud-centric IoT [2].

In [3], based on the requirements of the sensing objects, the authors propose deployment, development, and management of the IoT applications over the cloud, namely, the CloudThings architecture. Applications that can be improved by the integration of IoT into cloud computing are many; such as pervasive healthcare [4], smart homes [5], smart cities [6], and future transportation systems [7]. Furthermore, public safety in smart city management can be efficiently addressed by taking advantage of cloud and IoT integration [8]–[10]. In a cloud-centric IoT framework, sensors provide their sensed data to a storage cloud as a service, which then undergoes data analytics and data mining tools for information retrieval and knowledge discovery.

Built-in sensors in mobile devices can leverage the performance of IoT applications in terms of energy and communication overhead savings [11], [12]. Therefore, Sensing-as-a-Service (S^2aaS) appears as a strong candidate for front-end access to the cloud-centric IoT, where mobile devices provide their sensed data based on the pay-as-you-go fashion [13].

In this paper, we present a cloud-centric IoT-based crowd management scheme for public safety which utilizes S^2aaS with the ultimate goal of trustworthy crowdsourcing. The proposed scheme is called Trustworthy Sensing for Crowd Management (TSCM) which has been briefly presented in [14] with initial simulation results. As integration of S^2aaS and social networks can introduce various benefits to both systems [15], we present the TSCM framework with the option of social network assistance. TSCM enables the public safety authority to collect sensing data in a particular region for crowd management. The term crowd refers to a large group of people who have gathered for an event. Public safety authority can use sensor data of the smart phones if effective incentives exist for the users in the event to provide their sensing data as a service. TSCM adopts the MSensing auction-based user-centric incentives that have been proposed in [16] for a smart phone-based crowdsourcing scenario, and enhances them by introducing reputation-awareness and trustworthiness of the smart phone users. Maliciously altered sensing data aiming at disinformation at the public safety authority or inaccurate sensor readings reduce user reputation, whereas truthful and accurate sensor readings increase user trustworthiness.[1] TSCM uses recent and past sensor readings of a user in order to compute his/her current trustworthiness dynamically. As TSCM runs an auction to select the users who will crowdsource the required tasks, a user's bid and his/her marginal values introduced to the sensing set are redefined by the public safety authority by using the trustworthiness of the corresponding user. We show that when TSCM is adopted, the utility of the public safety

Manuscript received October 31, 2013; revised May 20, 2014; accepted June 29, 2014. Date of publication July 10, 2014; date of current version August 07, 2014.

The authors are with the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada (e-mail: kantarci@site.uottawa.ca; mouftah@site.uottawa.ca).

Digital Object Identifier 10.1109/JIOT.2014.2337886

[1]Hereafter, we use the terms, reputation and trustworthiness interchangeably.

authority is significantly improved by reputation-awareness, whereas disinformation probability in a crowdsourced task is dramatically reduced when compared to the reputation-unaware user-centric incentive approach. Furthermore, public safety authority can save 40% of the payments made to the malicious users in comparison to a reputation unaware auction.

This paper is organized as follows. In Section II, related work and motivation are presented. Section III presents the proposed framework, TSCM in detail. Numerical results are presented and discussed in Section IV. Section V concludes the paper and gives future directions.

II. Related Work and Motivation

In [17], the authors define the cloud as the front-end of the IoT architecture. IoT sensors are not necessarily to be stand alone forming wireless sensor network (WSN) clouds, but are mostly built-in sensors in mobile devices providing crowdsourcing-based sensing data. In order to address this issue, Pereira *et al.* [18] propose a service-oriented architecture (SOA) which utilizes constrained application protocol (CoAP) to exchange sensor and actuator data over the Internet. The proposed SOA consists of a web interface for the applications that monitor, configure, and visualize the sensor and actuator data.

In [19], an aggregation framework for WSNs has been presented in order to provide sensing and actuation clouds as a service. In [20], a different cloud-centric model has been introduced where sensors are virtualized in order to be shared among the end users over the cloud. A specific application of cloud-based crowdsourcing has been presented in [21], where a content-centric vehicular network model in a vehicular cloud has been proposed. In [22], the authors define S^2aaS in the IoT architecture as a 4-layer business model which consists of sensor devices and users, sensing data publishers, cloud service providers, and S^2aaS customers. We use this definition as a basis to our framework in the following sections. In [23], the authors have proposed a context-aware ranking system for selecting the sensing devices. A detailed survey on the state-of-the-art and challenges in S^2aaS has been presented in [15].

As smart devices have become widespread, crowdsourcing via social networks by off-the-shelf sensors in smart devices has become possible. In [15], the authors state that integration of social networks into S^2aaS would introduce several benefits to S^2aaS customers, as well as social network service users.

As stated in [24], IoT is the enabler for device-to-device communications whereas the social networks provide human-to-device communication in this integrated architecture, and they can enable connecting to ubiquitous computing environments. On the other hand, integration of social networking services into cloud-centric IoT is still an open issue although there are few studies which may be considered under this category. In [25], the authors have proposed a community detection algorithm for an integrated IoT and social network environment. Miluzzo *et al.* [26] have proposed the CenceMe application which uses built-in sensors in the smart phones to sense users' body positions and publish the information on their social networks in Facebook and/or MySpace. Besides, crowdsourced weather information and noise mapping as S^2aaS applications over Twitter have been proposed in [27].

S^2aaS calls for effective incentive mechanisms in order to ensure users' willingness to share their sensing data [15].

Previous work reports that user-centric local-search-based auction is vulnerable to untruthful bidding of the users who aim at increasing their incomes by participating the auction with higher bids. This vulnerability has been addressed by MSensing auction [16]. In the same study, MSensing has been shown to improve platform and user utility along with truthfulness in mobile phone-based crowdsourcing. Therefore, it can be adopted by a cloud-centric IoT framework, where S^2aaS forms the front-end. When such a framework is used for crowd management, users aiming at disinformation can cause more severe problems in public safety when compared to the users aiming at increasing their incomes by higher bids. Thus, malicious users participate the auction with lower bids, guarantee to be selected in an auction, and when selected, send altered data to the sensor data publisher layer of the IoT. In such a scenario, public safety authority may request several types of sensor data such as temperature, noise, motion, and image; and sensing services are provided by the crowd which consists of people who have gathered for a particular event. This vulnerability can be addressed by a reputation-aware crowd management scheme for a truthful and trustworthy S^2aaS in a cloud-centric IoT architecture.

III. Trustworthy Sensing for Crowd Management

A. System Architecture

The four layers of a cloud-centric IoT, see [22], correspond to four main components of TSCM as follows.

1) Crowd Management Authority: Submits sensing task requests to the cloud platform and receives the sensing data of the corresponding tasks once the auction is completed in the cloud. Indeed, sensing task requests also include the value of each task so that the cloud platform can manage the auction by jointly considering the utility of the crowd management authority, as well as the users' utility.

2) Cloud Computing Platform: Maintains a user database, where users' reputations, bids, payments, sensing tasks, and associated events are stored. Furthermore, the cloud platform interacts with social networking services in order to detect candidate users and collect sensing data. Huge amount of data will need to be stored and processed throughout an event; hence TSCM over Hadoop MapReduce framework can be a feasible solution for implementation.

3) Social Networking Service: Is considered to be the sensor data publisher layer in the cloud-centric IoT for crowd management. Furthermore, social network services can cooperate with the cloud platform in retrieving the users who are present at a particular location to attend a particular event. Moreover, S^2aaS data such as bids, payments, and sensing data are also published over social network, whereas the above

applications enable fast detection of the smart phone users who may take part in the S^{2}aaS auction.

4) Smart Phone Users: Denote a subset of the crowd in a particular region, which is aimed to be monitored by the public safety authority. A user who agrees to publish his/her sensing data on the sensor data publisher layer (e.g., social network) of the IoT architecture, installs the S^{2}aaS application on his/her smart phone. As mentioned in the motivation section, two types of users are considered in this scenario. The first type of users bid and publish their sensor data truthfully (i.e., nonmalicious users) whereas the second type of users bid lower than their costs in order to guarantee being selected, and publish altered sensing data in order to lead to disinformation at the public safety authority (i.e., malicious users).

TSCM consists of the following steps.

Step 1) Crowd management authority submits its S^{2}aaS request to the cloud platform.

Step 2) The cloud platform queries the users who have checked-in nearby corresponding location. Social networks respond with a list of candidate users who will join the auction.

Step 3) The cloud platform updates the user database and sends the tasks to the users via corresponding social networks.

Step 4) The users publish the sensing tasks in which they are interested on their social networks along with their corresponding bid values, and the social network relays the data to the cloud platform. It is worthwhile noting that the bid of a truthful user is equal to his/her sensing cost.

Step 5) The cloud platform runs the auction. First, it queries the database to retrieve user reputations. Once the user reputations are retrieved, the cloud platform selects the winners of the auction, determines the payments and sends user-task matching information along with the payments to the users via corresponding social network services.

Step 6) Users publish their sensing data on their social networks, which is also visible to the cloud platform.

Step 7) Upon receiving the sensing data, the cloud platform updates its user database with the newly calculated trustworthiness of the selected users. While calculating the trustworthiness of the users, the platform runs an outlier detection algorithm [28] to detect possibly altered data so that trustworthiness of the users who have sent altered data is degraded.

Step 8) The cloud platform sends the sensed data of the submitted tasks to the public safety authority.

B. Auction Mechanism

The auction mechanism in Steps 6 and 7 of TSCM adopts MSensing auction in [16] and enhances it by introducing reputation-awareness. The auction aims at selecting W winners out of P participants, and determining the payment to be made to each user i (ρ_i). Table I presents the notation used in the model. Among these terms, marginal value of user i for set W ($\vartheta_i(W)$) is a key parameter of the algorithm, and it denotes the additional value added to the corresponding set by the sensing tasks of user i as shown in (1). Value of a set ($\vartheta(W)$) denotes the total value of the tasks sensed by the users forming the corresponding set as shown in (2), where T_W is the list of tasks sensed by the users in set W. Since TSCM introduces reputation-awareness to MSensing auction, we also use the reputable marginal value ($\vartheta_i^{\Re}(W)$) of user i on set-W as formulated in (3). Reputable marginal value denotes the additional value introduced by user i to the reputable value of set W. Equation (4) formulates the reputable value of set-W which is calculated by summing the values of the tasks forming the sensing set while the value of a task is defined by its actual value scaled by the average trustworthiness of the users participating in the corresponding sensing task

TABLE I
NOTATION USED IN THE FORMULATION

Notation	Explanation
P (W):	Set of users (winners) participating S^{2}aaS
$\Re_i(t)$:	Trustworthiness of user i at time period t
$\Re_i$:	Overall trustworthiness of user i
$\vartheta(W)$:	Total value of the sensing tasks handled by the users in W
$\vartheta^{\Re}(W)$:	Reputation-based value of the sensing tasks handled by the users in W
$\vartheta_i^{\Re}(W)$:	Reputable marginal value of the user on the set W
b_i (c_i):	Bid (Cost) of the user i
ρ_i:	Payment to user i
Ω:	Reputation list
Φ:	Payments list
T:	Set of tasks
T_S:	Set of tasks handled by the users in the set S
T_i:	Set of tasks handled by user i
ϑ_t:	Value of task t
Γ_t:	Set of users handling task t

$$\vartheta_i(W) = \vartheta(W \cup \{i\}) - \vartheta(W) \tag{1}$$

$$\vartheta(W) = \sum_{t \in T_W} \vartheta_t \tag{2}$$

$$\vartheta_i^{\Re}(W) = \vartheta^{\Re}(W \cup \{i\}) - \vartheta^{\Re}(W) \tag{3}$$

$$\vartheta^{\Re}(W) = \sum_{t \in T_W} \sum_{j \in \Gamma_t} \vartheta_t \cdot \Re_j / |\Gamma_t|. \tag{4}$$

We define the trustworthiness of a user during the period t as the ratio of the positive readings ($p(t)$) to the total readings as $\Re_j(t) = (p(t) + \epsilon)/(p(t) + n(t) + \epsilon)$. When the cloud platform detects a sensor reading as an outlier, the corresponding sensor reading is marked as a negative reading (n).

Equation (5) is used to calculate the overall trustworthiness of a user ($\Re_i$), where latest and previous trustworthiness values [i.e., $\Re_j(t)$, $\Re_j^-$] contribute to the overall trustworthiness with β and α coefficients, respectively, where $\alpha + \beta = 1$. Thus, the greater the α (β) is, the less the contribution of the latest (previous) reputation is, and vice versa

$$\Re_j = \beta \cdot \Re_j(t) + \alpha \cdot \Re_j^-. \tag{5}$$

The auction has two modes, namely, the *aggressive* and *nonaggressive* modes. We also define an *adaptive* mode, where TSCM dynamically switches between these two modes and

Algorithm 1 Pseudocode of the Auction Mechanism in TSCM

1: **Begin**
2: $\{W \leftarrow \phi\ \}$
3: $\{i \leftarrow \arg\max_{p \in P} \{\vartheta_p^{\Re}(W) - b_p/\Re_p\}\}$
4: **while** $b_i/\Re_i < \vartheta_i^{\Re}$ **do**
5: $W \leftarrow W \cup \{i\}$
6: $i \leftarrow \arg\max_{p \in P \setminus W} \{\vartheta_p^{\Re}(W) - b_p/\Re_p\}$
7: **end while**
8: //Winners of the auction are found
9: **for all** $p \in P$ **do**
10: $\rho_p \leftarrow 0$
11: **end for**
12: **for all** $w \in W$ **do**
13: $P' \leftarrow P \setminus \{w\},\ \Delta \leftarrow \phi$
14: **repeat**
15: $w_v \leftarrow \arg\max_{v \in P' \setminus \Delta} \{\vartheta_v^{\Re}(\Delta) - b_v/\Re_v\}$
16: $\theta \leftarrow \min\left\{\vartheta_w^{\Re}(\Delta) - (\vartheta_{w_v}^{\Re}(\Delta) - b_{w_v}), \vartheta_w^{\Re}(\Delta)\right\}$
17: $\rho_w \leftarrow max(\rho_w, \theta)$
18: $\Delta \leftarrow \Delta \cup \{w_v\}$
19: **until** $b_{w_v}/\Re_{w_v} \geq \vartheta_{w_v}^{\Re}$ or $\Delta = P'$
20: **if** $b_{w_v}/\Re_{w_v} < \vartheta_{w_v}^{\Re}$ **then**
21: $\rho_w \leftarrow max(\rho_w, \vartheta_w^{\Re}(\Delta))$
22: **end if**
23: **end for**
24: $Outlier\_Detection(W)$;
25: **for all** $w \in W$ **do**
26: $update(\Re_w)$
27: **end for**
28: **return** (W, Φ, Ω)
29: **End**

adjusts the α and β parameters. We define each mode in the following three sections.

C. TSCM-Aggressive Mode

Algorithm 1 presents the service provisioning step in TSCM focusing on the two main auction steps, namely, the winner selection and payment determination.

1) Winner Selection: The algorithm starts with a set of winners which is initially empty (line-2). Between line-3 and line-7, the platform sorts the users with respect to their reputable marginal contributions. It is worthwhile noting that the users have already joined the auction by sending their bids to the platform. Thus, between line-3 and line-7, the algorithm selects the users whose modified bids are less than their reputable marginal values as the winners of the auction. Each winner is immediately added to the winners list (line-5). By modified bid, we denote the actual bid of a user scaled by his/her reputation. The idea behind using the modified bid of a user is increasing the selection probability of a user with a lower bid and higher reputation in comparison to the other users. Thus, a user with higher *reputable* contribution to the platform's utility is close to the head of the list, whereas a user with less contribution is close to the tail of the list, i.e., $(\vartheta_i^{\Re} - b_i/\Re_i) > (\vartheta_{i+1}^{\Re} - b_{i+1}/\Re_{i+1})$.

Algorithm 2 Payments in TSCM-Nonggressive Mode

1: P: Participants of the auction.
2: W: Winners of the auction.
3: **for all** $p \in P$ **do**
4: $\rho_p \leftarrow 0$
5: **end for**
6: **for all** $w \in W$ **do**
7: $P' \leftarrow P \setminus \{w\},\ \Delta \leftarrow \phi$
8: **repeat**
9: $w_v \leftarrow \arg\max_{v \in P' \setminus \Delta} \{\vartheta_v(\Delta) - b_v/\Re_v\}$
10: $\theta \leftarrow \min\left\{\vartheta_w(\Delta) - (\vartheta_{w_v}(\Delta) - b_{w_v}), \vartheta_w(\Delta)\right\}$
11: $\rho_w \leftarrow max(\rho_w, \theta)$
12: $\Delta \leftarrow \Delta \cup \{w_v\}$
13: **until** $b_{w_v} \geq \vartheta_{w_v}$ or $\Delta = P'$
14: **if** $b_{w_v} < \vartheta_{w_v}$ **then**
15: $\rho_w \leftarrow max(\rho_w, \vartheta_w(\Delta))$
16: **end if**
17: **end for**

2) Payment Determination: In the payment determination phase, similar to the benchmark scheme in [16], TSCM ensures that any user, user w, will not be paid less than his/her bid. Initially, each user is assumed to be paid zero (lines 9–11). For each selected user, user w, the algorithm constructs a temporary set which is equal to the set of participants excluding user w. The algorithm aims at constructing a temporary winners set Δ, out of the temporary participants set, P' (lines 15–19). Line-16, line-17, and line-21 denote the steps regarding payment determination for user w. In these lines, TSCM seeks maximum possible value for the corresponding user's bid which enables selection of user w, instead of user w_v in the temporary winners set Δ, out of the temporary participants set P'. Here, user w_v denotes a user in the set of participants, whose reputable marginal value is greater than its modified bid. To this end, we sort the users in the set Δ with respect to their reputable contributions as formulated by

$$(\vartheta_{w_v}^{\Re} - b_{w_v}/\Re_{w_v}) > \vartheta_{w_v+1}^{\Re} - b_{w_v+1}/\Re_{w_v+1}. \tag{6}$$

Once the cloud platform receives the sensor data, it eliminates the inaccurate readings via an outlier detection algorithm (line-24), and runs (5) in order to update the users' trustworthiness values in the database (lines 25–27).

D. TSCM-Nonaggressive Mode

Nonaggressive mode of TSCM can be preferred to avoid possible cuts in the user incomes as the aggressive mode of TSCM uses modified bids and reputable marginal values of the users for the set of winners. As seen in Algorithm 2, nonaggressive mode of TSCM adopts the payment determination phase of MSensing auction in [16], where winner selection phase is the same as that in the aggressive mode. Thus, while constructing the temporary set of winners Δ, the algorithm uses the raw value of the set Δ (lines 9–15). On the other hand,

in the payment steps (i.e., lines 10 and 15), the actual bids of the users are used so that the payment to be made to user w is not scaled by his/her reputation. It is worthwhile noting that the aggressive mode of TSCM aims at ensuring trustworthiness and minimum payment to the malicious users, therefore it determines the payments by considering the collective (i.e., reputable) value of the tasks in a set rather than the raw value. Since reputable value of a set can be less than its raw value, nonmalicious users are expected to receive higher payments compared to the payments received under the nonaggressive mode. On the other hand, a malicious user who is selected as a winner can also be paid based on the bids and marginal values of the remaining users and his/her own marginal value on the corresponding set.

In the worst-case scenario, number of selected users (W) is equal to the number of users (P), where the algorithm has to go through both inner and outer loops between lines 14 and 19, $\Delta = P'$ and $|P-1|$ times, respectively. Furthermore, since for each task $t \in T_\Delta$, $\Gamma_t = |P-1|$, computation of the reputable value of Δ is $O(|P| \cdot |T_\Delta|)$. Therefore, runtime complexity of an auction is $O(|P|^3 \cdot |T_\Delta|)$. Based on the fact that $|T_\Delta| \ll P$, the complexity of the algorithm is $O(|P|^3)$.

E. TSCM-Adaptive Mode

The adaptive mode of TSCM aims at dynamic adjustment of the impact of recent and past reputation of the user by varying α and β coefficients in trustworthiness calculation. Furthermore, in the winner selection phase (see Algorithm 1), the algorithm first selects the users whose trustworthiness values have not been degraded. This step is followed by selection of the users whose trustworthiness values have been degraded in the most recent task assignment period. To this end, TSCM-adaptive mode redefines the reputable marginal value for all users as formulated in (8). Thus, if the trustworthiness of a user has not been degraded in the previous period, the reputable marginal value of the corresponding user for a given set W is set at the naive marginal value of the user for W. By naive marginal value, we denote the calculation in (2). Otherwise, user's reputation is taken into account in order to calculate his/her reputable marginal value for W, which is defined in (4)

$$\vartheta_i^{\Re}(W) = \begin{Bmatrix} \vartheta^{\Re}(W \cup \{i\}) - \vartheta^{\Re}(W) & \text{if } \Re_i \leq \Re_i^- \\ \vartheta_i(W) & \text{else} \end{Bmatrix}. \quad (7)$$

At the end of each task assignment period, before updating the reputation of user i, the algorithm checks the positive and negative readings of the corresponding user in that period, and if user has reported more negative readings, the coefficient α for user i is decremented by α_{step}. Thus, while calculating the reputation of a user who has reported negative readings, contribution of his/her previous reputation to the current trustworthiness is degraded, as well. Otherwise, α_{step} is increased by α_{step} in order to disable trustworthiness of the user to increase rapidly (9). Indeed, adjustment of α_{step} is limited to a predefined interval which is bounded by $\alpha_{\min}$ and $\alpha_{\min}$. This process is formulated in

$$\alpha_i = \begin{Bmatrix} \max(\alpha_{\text{i}} - \alpha_{\text{step}}, \alpha_{\min}) & p_i(t) < n_i(t) \\ \min(\alpha_{\text{i}} + \alpha_{\text{step}}, \alpha_{\max}) & \text{else} \end{Bmatrix}. \quad (8)$$

IV. Numerical Results

A. Simulation Settings

We evaluate the TSCM framework in a 1000 m $\times$ 1000 m region in which 1000 participants are uniformly distributed during a 30-min event. It is assumed that the users already have the application installed on their smart phones. Certain amount of participants are assumed to be malicious users aiming at disinformation at the public safety authority. We assume that the built-in sensors of smart phones provide highly accurate readings at the order of 0.97–0.98 [29]. In each simulation scenario, public safety authority sends λ task requests to the social networking service every minute. Sensing tasks are also uniformly distributed over the terrain. Each user is interested in a task within his/her 30-m radius, and the value of a task varies between 1 and 5, whereas a user bid takes a value in $[1, 10]$ [16].

Since malicious users aim at disinformation at the crowd management authority, they participate the auction by bidding lower than their cost. Therefore, we assume that malicious users aggressively aim at winning in the auction; hence a malicious user bids 0.1 times of his/her cost. On the other hand, since the platform selects the users based on their trustworthiness, it is likely for a malicious user not to be selected once his/her trustworthiness is degraded to an extremely low value. This situation may occur if malicious users continuously publish altered sensing data on their social network, and this type of behavior is called *continuous disinformation (CD)*.

In order to keep his/her reputation at a level which may enable him/her to be reselected, a malicious user may keep track of his/her activity in order to compute his/her trustworthiness. Thus, he/she sends unaltered sensor readings until he/she ensures that his/her trustworthiness exceeds a threshold, UP_THRESHOLD. At this point, the user starts publishing altered sensing data over his/her social network aiming at disinformation at the public safety authority. As the public safety authority will start degrading, the corresponding user's trustworthiness, a malicious user who finds his/her trustworthiness below a threshold, DOWN_THRESHOLD, aims at increasing his/her trustworthiness, and restarts sending unaltered sending data. In the simulations, we set UP_THRESHOLD and DOWN_THRESHOLD at 0.8 and 0.5, respectively. We denote this type of behavior by *intermittent disinformation (ID)*.

Performance metrics are defined as follows: Utility of the public safety authority is the difference between the total reputable value of the sensing tasks and the total payments made to the winners in the auction as formulated in (9), where τ denotes the τth period in which the crowd management authority requested a new set of tasks through the cloud platform. Average user utility is the difference between total payments made to the winners and the total sensing cost of

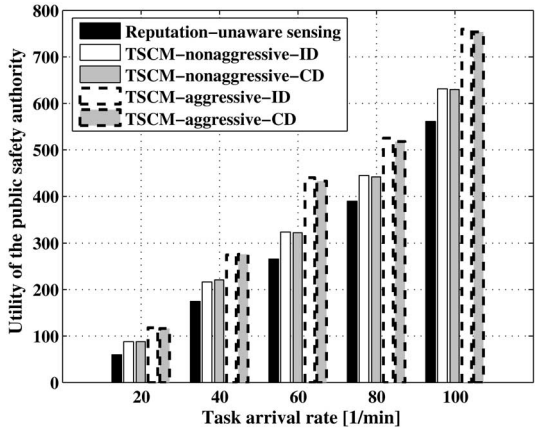

Fig. 1. Utility of the crowd management authority.

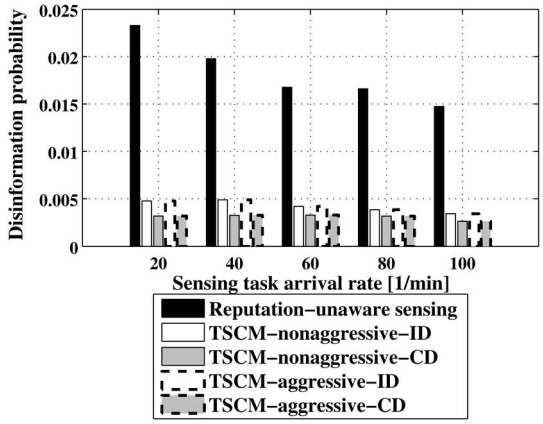

Fig. 2. Average DIR.

the winners as formulated in (10). Disinformation ratio (DIR) is the ratio of the tasks for which at least one malicious user has been paid to the total number of tasks [see (11)]

$$U_{\text{auth}} = \sum_{\tau}\left(\sum_{t\in T_{W_\tau}} \vartheta^{\tau}(W_\tau) - \sum_{i} {\rho_i}^{\tau}\right) \tag{9}$$

$$U_{\text{user}} = \left(\sum_{\tau}\left(\left(\sum_{i} {\rho_i}^{\tau} - \sum_{i} {c_i}^{\tau}\right)/|W_\tau|\right)\right)/\tau_{\text{end}} \tag{10}$$

$$\text{DIR} = \left(\sum_{\tau}\left(\sum_{t\in T_W^{\tau}}\sum_{i\in\Gamma_t}\text{sgn}(\rho_i)\right)/|T_W|\right)/\tau_{\text{end}}. \tag{11}$$

B. TSCM Performance Versus Reputation-Unaware Sensing

We first set the malicious user ratio at 0.05 and $\alpha = \beta = 0.5$ in order to equally treat a user's current and past reputation. In Fig. 1, we illustrate the utility of the public safety authority under TSCM and reputation-unaware sensing. Reputation-awareness introduces an increase of 12% to the utility of the public safety authority under lightly arriving sensing task requests, whereas enhancement in the utility of the public safety authority raises up to 85% under heavily arriving sensing task requests and the aggressive mode. In an auction, for the users with lower trustworthiness, the likelihood of being selected is low even though their original bids are lower than the other users. Furthermore, the aggressive mode of TSCM improves the performance of nonaggressive mode by approximately 15%. The aggressive mode determines the payments based on the reputable values of the task sets; hence, it leads to cuts in the payments made to the users with lower reputation (either malicious or nonmalicious). Furthermore, TSCM is robust to the ID strategy of the malicious users as the utility of the public safety authority is not significantly impacted when disinformation occurs intermittently rather than occurring continuously. In case of ID, the users improve their trustworthiness by temporarily publishing truthful information on their social network.

Fig. 2 illustrates the DIR under TSCM and reputation-unaware sensing. TSCM improves the benchmark scheme in terms of DIR by around 75%. Trustworthiness-based ranking

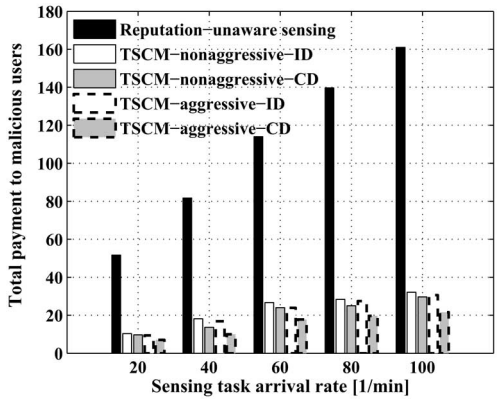

Fig. 3. Total payment to malicious users.

of the users reduce the likelihood of a malicious user to win in the auction. Besides, the public safety authority experiences higher DIR under ID in comparison to the case under CD. A malicious user with the ID strategy publishes unaltered data until its trustworthiness exceeds the UP_THRESHOLD. Then, the user resumes publishing altered data on its social network. Therefore, TSCM under ID experiences higher DIR.

As seen Fig. 3, TSCM leads to a significant reduction in payments made to the malicious users by up to 80%. Under the CD case and the aggressive mode of TSCM, minimum payments to the malicious users are made. However, even in the nonaggressive mode, TSCM can introduce savings over 70% in the payments made to the malicious users.

Fig. 4 reports that the improvement in the utility of the public safety authority, savings in the payments to the malicious users, and improvement in DIR are at the expenses of reduction in user utility. However, when compared to the improvement ratio in other performance metrics (Figs. 1–3), the reduction in user utility is significantly low. Furthermore, when sensing task requests arrive more frequently, the degradation in user utility is as low as 2% under the nonaggressive mode. Since every selected user is ensured to be paid at least his/her actual bid, slight degradation in user utility is acceptable.

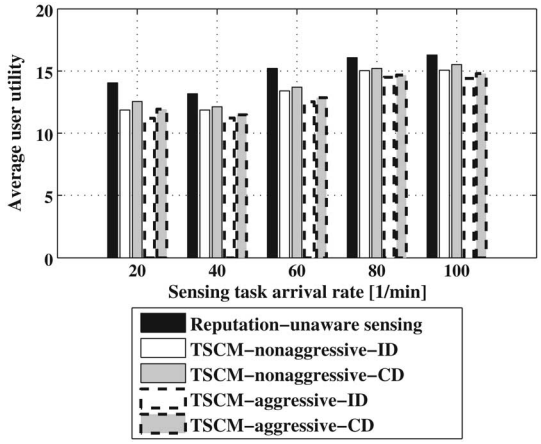

Fig. 4. Average utility of a participant.

C. TSCM Performance and Malicious Users Ratio

In Fig. 5(a), utility of the public safety authority is illustrated for TSCM-nonaggressive mode with ID. Under each load level, introducing reputation-awareness to crowdsourcing increases the platform utility as the ratio of malicious users increases. The enhancement in presence of significant amount of malicious users is more visible under heavy loads, where load denotes the sensing task request arrival rate.

Fig. 5(b) illustrates the total payment to the malicious users. In compliance with the previous figure, as the amount of malicious users increases, the benefits of TSCM is more clear as reputation-awareness avoids rapid selection of malicious users in the auction.

Fig. 5(c) illustrates the disinformation probability under various malicious user ratios. As users with low reputation are less likely to be selected, disinformation probability can be degraded by reputation-awareness. On the other hand, since reputation-unaware sensing does not discriminate users in the auction with respect to their trustworthiness, as the amount of malicious users increase, it makes the public safety authority become more prone to disinformation.

D. TSCM-Adaptive Mode and Impact of Coefficients

We simply set the ratio of malicious users at 0.05, and run TSCM in nonaggressive mode by setting α at 0.3, 0.5, and 0.7. Furthermore, we test the adaptive mode of TSCM which dynamically adjusts the coefficients.

Fig. 6(a)–(c) illustrates the utility of the public safety authority, total payments made to malicious users and disinformation probability, respectively. Setting α at a low value leads to better performance in comparison to the results under higher α values. The reason of this behavior is that the lower the α is, the higher the contribution of the current reputation of the user is. Hence, any negative reading of a user is expected to introduce drastic degradation in his/her reputation. Thus, the corresponding user will be less likely to be selected in the next periods. However, this may lead to an unfair treatment to a nonmalicious user who has reported a negative

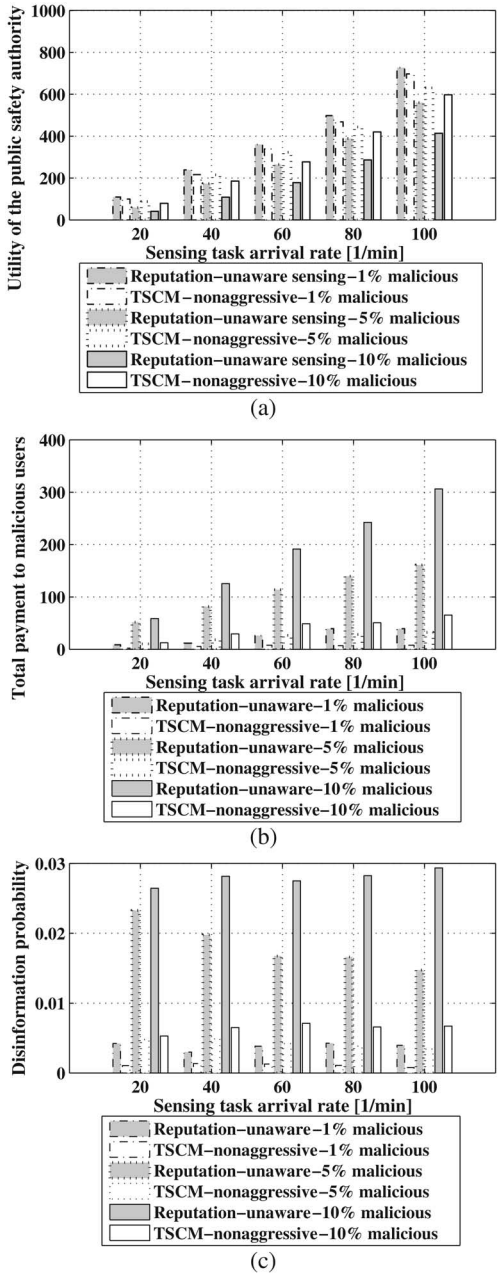

Fig. 5. Performance under various malicious user ratios: (a) utility of the safety authority, (b) total payment to malicious users, and (c) DIR.

reading due to several other factors. Setting α to higher values will not degrade the reputation of the user immediately, and the user will still have a chance to be selected in a future auction. Thus, the adaptive mode makes a compromise between the performances of TSCM under low and high α values.

Selection of the TSCM mode is based on the needs and priorities (i.e., platform utility and DR vs. user utility). TSCM-adaptive mode rectifies the dependency to the α parameter, and it can be adopted when the platform seeks compromise between platform utility and user utility, and aims at low disinformation probability.

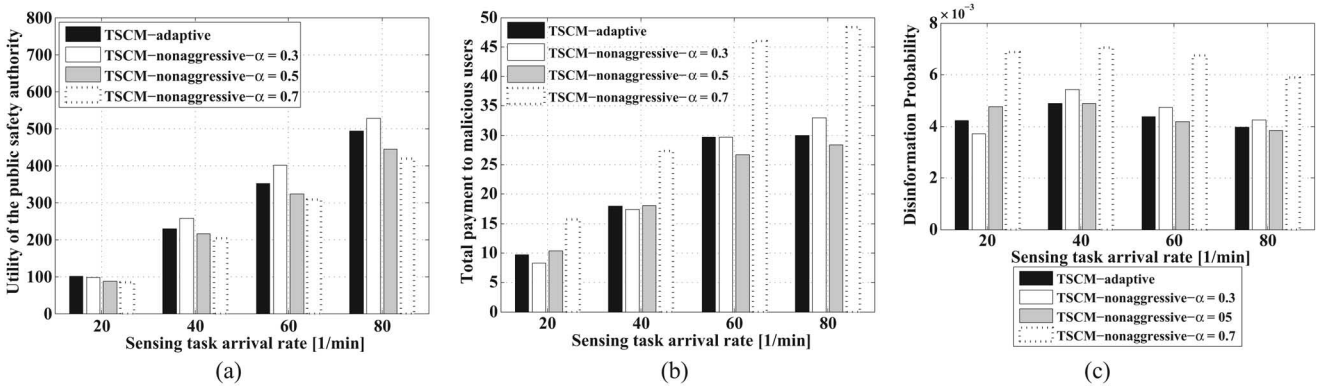

Fig. 6. Performance of TSCM under adaptive and various fixed reputation coefficients: (a) utility of the public safety authority, (b) total payment to the malicious users, and (c) DIR.

V. Conclusion

We have proposed a reputation-based framework for a cloud centric IoT architecture with the aim of crowd management, namely, TSCM. In TSCM, the cloud platform confirms the presence of the participants who are willing to collaborate with the public safety authority by publishing their sensing data and bids over their social networks. The cloud platform periodically updates the trustworthiness of users, which are used in assigning sensing tasks and making payments to the users. We have shown that utility of the public safety authority can be improved significantly, and the disinformation probability can be degraded by 75% by TSCM. Furthermore, the payments made to the malicious users who aim at disinformation at the public safety authority can be reduced by 40%. We have further shown that the adaptive mode of TSCM makes a compromise between utility of the public safety authority and tolerance to the inaccurate readings of nonmalicious users.

Early warning systems can utilize S^2aaS to assist disaster management [30]. Malicious groups may also use crowdsourcing to mislead the emergency forces [31] by injecting specious information into crowdsourced data. TSCM can also be adapted to such scenarios to increase community resilience against a crisis. Furthermore, integration of other trust derivation models [32] into TSCM can also enhance its efficiency.

References

[1] C. Aggarwal, N. Ashish, and A. Sheth, "The Internet of Things: A survey from the data-centric perspective," in *Managing and Mining Sensor Data*, C. C. Aggarwal, Ed. New York, NY, USA: Springer, 2013, pp. 383–428.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] J. Zhou *et al.*, "CloudThings: A common architecture for integrating the Internet of Things with cloud computing," in *Proc. IEEE 17th Int. Conf. Comput. Supported Cooperative Work Des. (CSCWD)*, Jun. 2013, pp. 651–657.

[4] C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," in *Proc. 6th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2012, pp. 922–926.

[5] S.-Y. Chen, C.-F. Lai, Y.-M. Huang, and Y.-L. Jeng, "Intelligent home-appliance recognition over IoT cloud network," in *Proc. 9th Int. Wireless Commun. Mobile Comput. Conf.*, Jul. 2013, pp. 639–643.

[6] G. Suciu *et al.*, "Smart cities built on resilient cloud computing and secure Internet of Things," in *Proc. 19th Int. Conf. Control Syst. Comput. Sci. (CSCS)*, May 2013, pp. 513–518.

[7] X. Yu, F. Sun, and X. Cheng, "Intelligent urban traffic management system based on cloud computing and Internet of Things," in *Proc. Int. Conf. Comput. Sci. Service Syst. (CSSS)*, Aug. 2012, pp. 2169–2172.

[8] W. Li, J. Chao, and Z. Ping, "Security structure study of city management platform based on cloud computing under the conception of smart city," in *Proc. 4th Int. Conf. Multimed. Inf. Netw. Security (MINES)*, Nov. 2012, pp. 91–94.

[9] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework for creating a smart city through Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 112–121, Apr. 2014.

[10] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[11] C. Perera, P. Jayaraman, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Dynamic configuration of sensors using mobile sensor hub in Internet of Things paradigm," in *Proc. IEEE Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process.*, Apr. 2013, pp. 473–478.

[12] A. E. Al-Fagih, F. M. Al-Turjman, W. M. Alsalih, and H. S. Hassanein, "A priced public sensing framework for heterogeneous IoT architectures," *IEEE Trans. Emerging Topics Comput.*, vol. 1, no. 1, pp. 133–147, Jun. 2013.

[13] X. Sheng, X. Xiao, J. Tang, and G. Xue, "Sensing as a service: A cloud computing system for mobile phone sensing," in *Proc. IEEE Sensors*, Oct. 2012, pp. 1–4.

[14] B. Kantarci and H. T. Mouftah, "Reputation-based sensing-as-a-service for crowd management over the cloud," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. SAC-P1.1–SAC-P1.6.

[15] X. Sheng, J. Tang, X. Xiao, and G. Xue, "Sensing as a service: Challenges, solutions and future directions," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3733–3741, Oct. 2013.

[16] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing," in *Proc. 18th Int. Conf. Mobile Comput. Netw.*, Aug. 2012, pp. 173–184.

[17] B. B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, "Cloud computing for Internet of Things and sensing based applications," in *6th Int. Conf. Sens. Technol. (ICST)*, Dec. 2012, pp. 374–380.

[18] P. P. Pereira *et al.*, "Enabling cloud connectivity for mobile Internet of Things applications," in *Proc. IEEE 7th Int. Symp. Service Oriented Syst. Eng. (SOSE)*, Mar. 2013, pp. 518–526.

[19] S. Distefano, G. Merlino, and A. Puliafito, "Sensing and actuation as a service: A new development for clouds," in *Proc. 11th IEEE Int. Symp. Netw. Comput. Appl. (NCA)*, 2012, pp. 272–275.

[20] R. Di Lauro, F. Lucarelli, and R. Montella, "SIaaS—Sensing instrument as a service using cloud computing to turn physical instrument into ubiquitous service," in *Proc. IEEE 10th Int. Symp. Parallel Distrib. Process. Appl. (ISPA)*, Jul. 2012, pp. 861–862.

[21] P. Talebifard and V. C. M. Leung, "Towards a content-centric approach to crowd-sensing in vehicular clouds," *J. Syst. Archit.*, vol. 59, no. 10, pp. 976–984, 2013.

[22] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by Internet of Things," *Trans. Emerging Telecommun. Technol.*, vol. 25, no. 1, pp. 81–93, Jan. 2014.

[23] C. Perera *et al.*, "Sensor search techniques for sensing as a service architecture for the Internet of Things," *IEEE Sensors J.*, vol. 14, no. 2, pp. 406–420, Apr. 2014.
[24] A. M. Ortiz, D. H. Ali, S. Park, S. N. Han, and N. Crespi, "The cluster between Internet of Things and social networks: Review and research challenges," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 206–215, Jun. 2014.
[25] S. Misra, R. Barthwal, and M. S. Obaidat, "Community detection in an integrated Internet of Things and social network architecture," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 1647–1652.
[26] E. Miluzzo *et al.*, "Sensing meets mobile social networks: The design, implementation and evaluation of the CenceMe application," in *Proc. ACM Conf. Embedded Netw. Sensor Syst.*, 2008, pp. 337–350.
[27] Y. S. Yilmaz, M. F. Bulut, C. G. Akcora, M. A. Bayir, and M. Demirbas, "Trend sensing via Twitter," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 14, no. 1, pp. 16–26, 2013.
[28] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 2, pp. 159–170, 2nd Quarter 2010.
[29] Y. He and Y. Li, "Physical activity recognition utilizing the built-in kinematic sensors of a smartphone," *Int. J. Distrib. Sensor Netw.*, vol. 2013, 2013, doi:10.1155/2013/481580.
[30] P.-H. Tsai, Y.-J. Lin, Y.-Z. Ou, E.T.-H. Chu, and J. W. S. Liu, "A framework for fusion of human sensor and physical sensor data," *IEEE Trans. Syst. Man Cybern. Syst.*, May 2014, doi: 10.1109/TSMC.2014.2309090.
[31] A. C. Weaver, J. P. Boyle, and L. I. Besaleva, "Applications and trust issues when crowdsourcing a crisis," in *Proc. 21st Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2012, pp. 1–5.
[32] J. Duan, D. Gao, D. Yang, C. H. Foh, and H. Chen, "An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 58–69, Feb. 2014.

Burak Kantarci (S'05–M'09–SM'12) received the M.Sc. and Ph.D. degrees in computer engineering from Istanbul Technical University, Istanbul, Turkey, in 2005 and 2009, respectively.

He is a Postdoctoral Researcher with the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada. From 2007 to 2008, he was a Visiting Scholar with the School of Information Technology and Engineering, University of Ottawa, where he completed the major content of the Ph.D. thesis. He has coauthored over 80 technical papers in established journals and flagship conferences, and he has contributed to eight book chapters. He coedited *Communication Infrastructures for Cloud Computing* (IGI Global, 2013).

Dr. Kantarci has served in the Technical Program Committee's several symposia of IEEE GLOBECOM and IEEE ICC conferences. He has cochaired the International Workshop on Management of Cloud Systems (MoCS) for three years. In 2005, he was the recipient of the Siemens Excellence Award for his contributions to optical burst switching research.

Hussein T. Mouftah (S'74–M'76–SM'80–F'90) joined the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada, in 2002, as a Tier 1 Canada Research Chair Professor, where he became an University Distinguished Professor in 2006. From 1979 to 2002, he was with the ECE Department, Queens University, Kingston, ON, Canada, where he was, prior to his departure, a Full Professor and the Department Associate Head. He possesses six years of industrial experience at Bell Northern Research of Ottawa, Ottawa, ON, Canada (now Nortel Networks). He has authored or coauthored of 9 books, 65 book chapters, more than 1300 technical papers, and 142 industrial reports. He holds 12 patents.

Dr. Mouftah served as an Editor-in-Chief of the *IEEE Communications Magazine* from 1995 to 1997, the IEEE ComSoc Director of Magazines from 1998 to 1999, the Chair of the Awards Committee from 2002 to 2003, a Director of Education from 2006 to 2007, a Member of the Board of Governors from 1997 to 1999 and 2006 to 2007, and a Member of the Nomination Committee since 2012. He has been a Distinguished Speaker of the IEEE Communications Society from 2000 to 2007. He has been a Fellow of the Canadian Academy of Engineering since 2003, the Engineering Institute of Canada since 2005, and the Royal Society of Canada (RSC) Academy of Science since 2008. He was a corecipient of 19 Best Paper and/or Outstanding Paper Awards. He was the recipient of numerous prestigious awards, such as the 2007 Royal Society of Canada Thomas W. Eadie Medal, the 2007–2008 University of Ottawa Award for Excellence in Research, the 2008 ORION Leadership Award of Merit, the 2006 IEEE Canada McNaughton Gold Medal, the 2006 EIC Julian Smith Medal, the 2014 EIC Y. K. Lo Medal, the 2004 IEEE ComSoc Edwin Howard Armstrong Achievement Award, the 2004 George S. Glinski Award for Excellence in Research of the University of Ottawa Faculty of Engineering, the 1989 Engineering Medal for Research and Development of the Association of Professional Engineers of Ontario (PEO), and the Ontario Distinguished Researcher Award of the Ontario Innovation Trust.