This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

Dynamic Trust Enforcing Pricing Scheme for Sensors-as-a-Service in Sensor-Cloud Infrastructure

Aishwariya Chakraborty†, *Student Member, IEEE*, Ayan Mondal†, *Student Member, IEEE*, Arijit Roy‡, *Student Member, IEEE*, and Sudip Misra†, *Senior Member, IEEE*

Abstract—In this paper, the problem of provisioning high quality of Sensors-as-a-Service (Se-aaS) in the presence of competitive sensor-owners, i.e., oligopolistic market, and heterogeneous sensor nodes in service-oriented sensor-cloud is studied. Oligopolistic sensor-owners adopt unfair means to degrade the quality of service provided by other sensor-owners in the sensor-cloud market. In order to address this problem, a dynamic pricing scheme, named DETER, is proposed in this work to enforce trust among the sensor-owners for maintaining the quality of Se-aaS provided by the Sensor-Cloud Service Provider (SCSP). Each sensor node calculates distributed trust opinion for other nodes, while the SCSP calculates centralized trust opinion for each sensor-owner. A Single-Leader-Multiple-Follower Stackelberg Game is formulated in which the SCSP acts as the leader and decides price to be paid to each sensor-owner, while ensuring maximum profit. On the other hand, the sensor-owners act as the followers and decide their strategies for earning maximum profit. Thereby, using DETER, SCSP enforces high trust among the sensor-owners. Additionally, using DETER, energy consumption of sensor nodes in sensor-cloud decreases by 4.69-11.56%, and network overhead decreases by 52.6-56.53%. The trade-off between price earned by the sensor-owners and profit of the SCSP in service-oriented sensor-cloud is also maintained using DETER.

Index Terms—Sensor-Cloud, Trust Enforcing, Dynamic Pricing, Oligopoly, Bi-Level Trust, Game Theory.

1 Introduction

For the development of a wireless sensor network (WSN)-based application, a user is generally required to purchase, deploy and maintain his/her own application-specific hardware resources. So, in order to relieve the users of WSN-based applications from the associated implementation complexities and financial expenditures, the *sensor-cloud* architecture was conceptualized [1]. Sensor-cloud basically follows a Service-Oriented Architecture (SOA). In sensor-cloud, the responsibilities of a user are shifted to a centralized *Sensor-Cloud Service Provider* (SCSP), which obtains WSNs on rental basis from multiple sensor-owners and provides these resources to the users in the form of chargeable units of services. The concept of resource virtualization of cloud computing is extended into WSNs to allow sharing of physical sensor nodes between multiple end-users, thereby allowing the provisioning of *Sensors-as-a-Service (Se-aaS)*. By transferring majority of the functionalities from the sensor nodes to the cloud, sensor-cloud reduces the computational burden as well as the resource consumption of each node, while increasing the overall network lifetime. Additionally, sensor-cloud also provides a platform for sensor-owners to increase the utilization of their hardware resources and earn profits by leveraging the same.

1.1 Motivation

Sensor-cloud provisions Se-aaS to the end-users and involves a flow of revenue from the end-users to the SCSP. In the competitive Se-aaS market, an SCSP needs to ensure proper pricing and quality of the delivered service. Chatterjee *et al.* [2] envisioned Se-aaS as a combination of both hardware and infrastructure services — heterogeneous SOA, unlike traditional cloud services. Hence, the existing pricing schemes designed for WSNs [3], [4] and cloud services [5], [6] are not suitable for sensor-cloud. On the other hand, for providing high quality-of-service (QoS) in sensor-cloud, it is indispensable for an SCSP to maintain accuracy or correctness of the data requested by an end-user. However, this issue is not addressed in the existing literature. In sensor-cloud, a fraction of the revenue earned by the SCSP is distributed among the sensor-owners for usage of their sensor nodes for sensing and relaying of sensed data based on centralized decision taken by the SCSP. This gives rise to an *oligopolistic market* scenario among the sensor-owners in the SOA of sensor-cloud. In sensor-cloud, the sensor-owner of the source node has to rely on

- † *Aishwariya Chakraborty, Ayan Mondal, and Sudip Misra are with the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India (Email: aishwariyachakraborty@gmail.com; ayanmondal@sit.iitkgp.ernet.in; smisra@sit.iitkgp.ernet.in).*
- ‡ *Arijit Roy is with the Advanced Technology Development Centre, Indian Institute of Technology Kharagpur, India (Email: arijitr@iitkgp.ac.in*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

the intermediate nodes, which are selected in a distributed manner, belonging to other sensor-owners to transmit the sensed data to the base-station (BS). In the process, these sensor-owners gain complete control over the sensed data. In such a situation, a selfish sensor-owner, who is driven solely by the urge to satisfy his/her self-interests, may adopt unfair means to reduce QoS. Thereby, the reputation of the honest sensor owner reduces, which in turn reduces the selection preference of the nodes belonging to him/her. This may eventually give rise to a monopoly situation. Additionally, the net profit incurred by the SCSP reduces. In the existing literature, few works exist on sensor-cloud, which include service-oriented pricing schemes, viz., [2]. However, none of these works considered the possibility of the aforementioned event. Hence, it is important to design a scheme, which is suitable for the sensor-cloud environment, in order to prevent such kind of monopoly situation from arising in oligopolistic market scenario of sensor-cloud.

Motivating Scenario: We consider a Sensor-Cloud Infrastructure (SCI) which is capable of providing environment monitoring services over an extensive geographic region. End-users, such as weather forecasting agencies, agricultural land owners, and industrial plants, do not need to purchase and deploy individual WSNs. Instead, they obtain the information of the environment condition in the form of Se-aaS. On the other hand, in order to provision Se-aaS, the SCSP relies on sensor nodes deployed by multiple sensor-owners in the concerned geographic region. Additionally, each sensor-owner depends on the other sensor-owners for transmitting sensed data from the sensor nodes to the BS via multihop communication, as mentioned earlier.

1.2 Contribution

In this paper, we introduce a *Single Leader Multiple Follower Stackelberg game theory*-based *dynamic trust enforcing pricing* (*DETER*) scheme for sensor-cloud, while considering that the sensor-owners form an oligopolistic market. In DETER, each sensor node in the path, from the source node to the BS, selects the set of most suitable next-hop nodes. Thus, DETER ensures an optimum trust value for the path and maintains the QoS of Se-aaS provided by the SCSP. Additionally, the proposed scheme, DETER, ensures the profit of both the SCSP and the sensor-owners. We refer to the optimal strategies chosen by each sensor node in the path obtained by using the DETER scheme as the Stackelberg equilibrium. In summary, the specific contributions of this work are given as follows:

a) We propose a dynamic trust enforcing pricing scheme for service-oriented sensor-cloud, while considering the possibility of selfish behavior by the sensor-owners.

b) In order to identify the misbehaving sensor-owners, we calculate distributed and centralized trust opinion sets for each owner using the beta reputation model proposed by Jøsang [7].

c) We use *Single Leader Multiple Followers Stackelberg game theoretic* approach for designing the proposed pricing scheme. In DETER, the SCSP acts as the leader, and the sensor-owners act as the followers.

d) We present four different algorithms to ensure QoS of Se-aaS, while choosing trust-enforced path for data transmission in service-oriented sensor-cloud.

2 Related Works

In the existing literature, few works focus on the integration of WSNs with the cloud, viz. [8], [9]. However, the concept of sensor-cloud was conceived by Yuriama *et al.* [9]. The authors [9] presented an overview of the entire architecture of sensor-cloud. Further, the theoretical modeling of sensor-cloud, along with characterization of the concept of virtualization of sensor nodes used in sensor-cloud, was presented by Misra *et al.* [1]. In another work, Bose *et al.* [10] studied the implementation of an infrastructure, which is suitable for environmental monitoring. Additionally, the practical implementation of sensor-cloud was demonstrated by Madria *et al.* [11]. Chatterjee *et al.* [12] studied an optimal composition of virtual sensors, while considering the resource-constrained behavior of the nodes. The problem of redundant data transmissions in sensor-cloud was explored by Chatterjee *et al.* [13], where a data caching mechanism between the sensor nodes and the cloud was suggested as a potential solution. In another work, Chatterjee *et al.* [14] addressed the problem of selecting the optimal data center using the optimal decision rule. Misra *et al.* [15] presented an optimal duty scheduling algorithm suitable for sensor-cloud environment.

On the other hand, some of the existing works consider the movement of data from the source node to the BS in the sensor-cloud environment. Misra *et al.* [16] studied the selection of the optimal gateway node for transmission of the sensed data to the cloud. In another work, Chatterjee *et al.* [17] proposed a scheme for selecting the optimal intermediate node for data transmission, while considering the unintentional node failures. Therefore, we argue that the problem of intentional misbehavior of sensor nodes or sensor-owners in sensor-cloud has not been explored yet in the existing literature. There exist several works in traditional WSNs, which consider the presence of misbehavior of sensor nodes. Illiano *et al.* [18] surveyed different schemes proposed for anomaly detection and trust management. Li *et al.* [19] proposed a trust-based system for clustered WSNs. Rezvani *et al.* [20] studied a trust-based scheme for secure aggregation of data using a modified iterative

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

filtering algorithm. In another work, Ahmed *et al.* [21] presented a-trust and energy-aware routing protocol for WSNs, while considering hop counts and load balancing of routes. However, it is also not suitable for a group of misbehaving nodes, which is a common scenario in sensor-cloud. Rathore *et al.* [22] proposed a consensus aware socio-psychological trust model to evaluate the trustworthiness of a node. However, these schemes are not suitable for using in the case of sensor-cloud, because of the following reasons:

a) Most of these works consider cluster-based and layered WSNs. The trust calculation process used varies based on cluster-heads and aggregators, which are assumed to be trustworthy. However, these are not suitable for sensor-cloud due to the presence of multiple sensor networks deployed by the different sensor-owners.

b) Most of the proposed schemes deal with homogeneous sensor nodes. However, sensor-cloud typically deals with heterogeneous sensor nodes, which are used for multitude of purposes.

c) Finally, in the existing literature, the proposed schemes aim to reduce the effects of the misbehavior of nodes on the sensed data. However, there is a need to prevent these situations from occurring, which is one of the primary objectives of this work.

Therefore, in contrast to the previous works, a game theory based dynamic trust enforcement pricing scheme, DETER, for SOA of sensor-cloud is proposed in this paper in order to prevent competitive sensor-owners from misbehaving and ensure QoS. The proposed scheme, DETER, exploits the economic aspects of the service-oriented sensor-cloud to encourage the sensor-owners to behave honestly.

3 System Model

We consider that the sensor-cloud has a few sensor-owners, as shown in Figure 1. Each sensor-owner $s_l \in \mathcal{S}$, where $\mathcal{S}$ is the set of the sensor-owners, is registered with the SCSP. The set of heterogeneous sensor nodes owned by each sensor-owner s_l is denoted by $\mathcal{O}_l$. In Figure 1, we denote heterogeneous sensor nodes using different geometrical shapes. We consider that the total set of sensor nodes registered with the SCSP is denoted by $\mathcal{N}$. Hence, we have, $\mathcal{N} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_{|\mathcal{S}|}$. On the other hand, each end-user u_r registers his/her service requirements with the SCSP, based on which a Service Level Agreement (SLA) [23], [24] is generated. The SLA states the service demanded by the user, and the agreed standards of various parameters such as — the maximum tolerable delay δ, and the maximum price $\mathcal{P}_{max}$ that the end-user is willing to pay for the service. We consider that the SCSP follows the dynamic 'pay-per-use' model, where the end-users pay based on their usage of the service provided by the SCSP.

Based on the requirement of end-user u_r, *virtual sensors*, denoted by vs_j, are formed by the SCSP for each application j using a subset of the physical sensor nodes $\mathcal{N}_j \subseteq \mathcal{N}$, and allocated to u_r. The set of virtual sensors assigned to each end-user u_r is denoted as $vg_r = \{vs_1, vs_2, \cdots, vs_p\}$, where p is the total number of applications requested by the end-user u_r. On the other hand, the selected source nodes sense and transmit their sensed data to the SCSP using a multi-hop path, as shown in Figure 2. The sensor nodes use nodes belonging to other sensor-owners as intermediate node. Thereby, the sensor-owners of the intermediate selected nodes earn revenue for providing services. Finally, the data is relayed to the cloud, where subsequent processing is performed to meet the end-user requirements. The list of symbols used in this work is mentioned in Table 1.

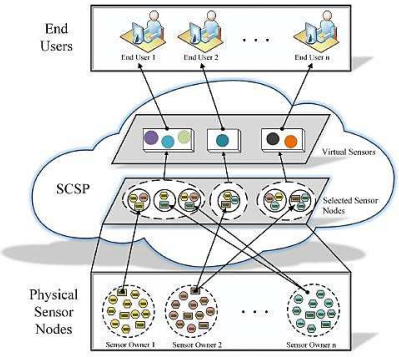

Fig. 1: Schematic Diagram of Sensor-Cloud

TABLE 1: List of Symbols

Symbol	Description
$\mathcal{S}$	Set of registered sensor-owners
$\mathcal{O}_l$	Set of sensor nodes of sensor-owner s_l
$\mathcal{N}$	Set of sensor nodes registered with SCSP
vs_j	Set of virtual sensors for application j
$\mathcal{N}_j$	Set of physical sensors mapped to vs_j
vg_r	Set of virtual sensors assigned to user u_r
$\mathcal{P}_{max}$	Maximum price willing to pay by user
φ	Profit earned by SCSP
δ	Maximum tolerable delay for a service
$\mathcal{P}^t_{path_g}$	Utility function of SCSP for $path_g$
$v^t_{n,i}$	Trust rating for node i by node n
$DO^t_{n,i}$	Distributed trust opinion set for node i
$\mathcal{M}^t_n$	Candidate set decided by n
$r^t_{n,i}, h^t_{n,i}$	Instantaneous feedback pair for node i
β	Forgetting factor
$R^t_{n,i}, H^t_{n,i}$	Cumulative feedback pair for node i
C^t_n	Centralized trust opinion set for node n
$\mathbb{D}^t_{scsp,i,n}$	Discounted trust opinion set
CO^t_l	Centralized trust opinion set for owner s_l
$U^t_{n,i}(\cdot)$	Utility function for node i
$EF^t_{n,i}$	Expectation Factor for node i
p^t_i	Pseudo-price for selecting next-hop
TE^t_l	Trust expectation of sensor-owner s_l

Assumptions: We list the assumptions considered in the design of the proposed scheme, DETER.

- The SCSP, which is a centralized entity, is responsible for maintaining the dynamic pricing policy.
- The set of source nodes, which are selected by the SCSP, transmit their sensed data to the cloud using different paths. No aggregation of data is performed by the intermediate nodes.
- Each node has a list of sensor nodes belonging to the same sensor-owner.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

- Each node is capable of overhearing, while being in the active or idle states [25], [26].

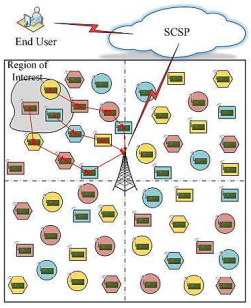

Fig. 2: Schematic Diagram of Sensor-Cloud with Heterogeneous Sensor Nodes

4 Proposed Dynamic Trust Enforcing Pricing (DETER) Scheme

The proposed scheme, DETER, comprises of two main components — *bi-level trust calculation*, which is performed periodically by the sensor nodes and the SCSP, and *dynamic pricing game*, which is conducted at the beginning of each service. The two components are discussed in details in the subsequent sections.

4.1 Trust Function Calculation

In this work, we propose a *bi-level trust factor calculation* method, which is motivated by the beta reputation model [7], and discounting and consensus operators [27], [28]. We consider dual trust values, defined as the *distributed trust opinion* (DO) and the *centralized trust opinion* (CO) sets. In the proposed scheme, DETER, at time instant $t \in \mathcal{T}$, each sensor node $n \in \mathcal{N}$ calculates the DO set, where $DO^t_{n,i} = (b^t_{n,i}, d^t_{n,i}, u^t_{n,i}, a^t_{n,i})$. $b^t_{n,i}$, $d^t_{n,i}$, $u^t_{n,i}$ and $a^t_{n,i}$ are defined as belief, disbelief, uncertainty, and atomicity, respectively, for the neighbor nodes, i.e., $\forall i \in N_n \subseteq \mathcal{N}$, where N_n denotes the set of neighbor nodes of sensor node n. It needs to satisfy the constraint — $b^t_{n,i}+d^t_{n,i}+u^t_{n,i} = 1$.

Eventually, these values become a key factor, for deciding the *candidate set ($\mathcal{M}^t_n$) of potential data forwarding nodes*, where $\mathcal{M}^t_n \subseteq N_n$. On the other hand, the SCSP calculates the centralized trust opinion set, i.e., $C^t_n = (b^t_{scsp,n}, d^t_{scsp,n}, u^t_{scsp,n}, a^t_{scsp,n})$, $\forall n \in \mathcal{N}$, using the discounting and consensus operators, while operating on the previous trust opinion set $C^{t-1}_n = (b^{t-1}_{scsp,n}, d^{t-1}_{scsp,n}, u^{t-1}_{scsp,n}, a^t_{scsp,n})$, and the set of opinions collected from the deployed sensor nodes. Here, we have $b^t_{scsp,n} + d^t_{scsp,n} + u^t_{scsp,n} = 1$. In the following subsections, we discuss the method of calculation of the DO and CO sets.

4.1.1 Distributed Trust Opinion Set

Each sensor node generates a DO set for each of its neighbor nodes, periodically. In order to calculate the DO set, the sensor nodes notice the packet forwarding behavior of their next-hop nodes by utilizing the property of overhearing. The steps of DO set calculation are listed as follows.

1) First, each node n calculates the *trust rating* $v^t_{n,i}$ for each node $i \in N_n$, as defined in Definition 1.

Definition 1. *At time instant t, the trust rating $v^t_{n,i}$ calculated by node n for node i is defined as the ratio of the number of correctly forwarded data packets $F^t_{n,i}$ by node i among those received from node n to the total number of packets $T^t_{n,i}$ sent to node i by node n.*

We assume that each node n has the information whether neighbor node $i \in N_n$ belongs to the same sensor-owner as itself. If neighbor node i belongs to the same sensor-owner, s_k, as node n, trust rating is considered to be 1. Mathematically,

$$v^t_{n,i} = \begin{cases} 1, & \text{if } \{n,i\} \in \mathcal{O}_k \text{ and } i \in N_n \\ \frac{F^t_{n,i}}{T^t_{n,i}}, & \text{otherwise} \end{cases} \quad (1)$$

2) Next, using the trust ratings, each node n determines the *instantaneous* positive and negative feedback parameters [7] for each neighbor node i at time instant t, i.e., $r^t_{n,i}$ and $h^t_{n,i}$, respectively, using the following equations:

$$(r^t_{n,i},\ h^t_{n,i}) = \left(\frac{w(1+v^t_{n,i})}{2}, \frac{w(1-v^t_{n,i})}{2}\right) \quad (2)$$

where w is defined by SCSP, and is a constant for node n, where $w > 0$.

3) Thereafter, the *cumulative* positive and negative feedback pair $(R^t_{n,i}, H^t_{n,i})$ is calculated by node n for each neighbor node i at time instant t, using the following equations:

$$(R^t_{n,i}, H^t_{n,i}) = (R^{t-1}_{n,i}\beta + r^t_{n,i}, H^{t-1}_{n,i}\beta + h^t_{n,i}) \quad (3)$$

where β is the *forgetting factor*, and is defined by the SCSP.

4) Finally, based on beta reputation model [7], each node n calculates $DO^t_{n,i}$ for neighbor node i as follows:

$$(b^t_{n,i}, d^t_{n,i}, u^t_{n,i}) = \left(R^t_{n,i}/K, H^t_{n,i}/K, 2/K\right) \quad (4)$$

where $K = (R^t_{n,i}+H^t_{n,i}+2)$. Additionally, we consider $a^t_{n,i} = \frac{1}{2}$, so that, uncertainty is equally distributed among belief and disbelief.

4.1.2 Centralized Trust Opinion Set

The SCSP calculates the CO set, C^t_n, for each sensor node $n \in \mathcal{N}$, i.e., $C^t_n = (b^t_{scsp,n}, d^t_{scsp,n}, u^t_{scsp,n}, a^t_{scsp,n})$, using the consensus and discounting operators [27]–[29] on the DO sets obtained from each node. Thereafter, the SCSP calculates the CO set for each sensor-owner $s_l \in \mathcal{S}$, CO^t_l, based on the calculated CO set

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

of each of its sensor node $n \in \mathcal{O}_l$. The steps for calculation of CO set for each sensor-owner by the SCSP are listed as follows:

1) Initially, the SCSP defines the CO set for each sensor node $n \in \mathcal{N}$ at time instant t_0 as $C_n^{t_0} = (1, 0, 0, 0.5)$. Thereafter, it collects the DO sets from the individual sensor node i for each of its neighbor nodes, $n \in N_i$, periodically.

2) Next, the SCSP calculates the *discounted opinion* of node n, i.e., $\mathbb{D}^t_{scsp,i,n}$, using its own opinion of node i in the previous time instant, C_i^{t-1} and the DO sets. Hence, $\mathbb{D}^t_{scsp,i,n}$ is determined as follows[1]:

$$\mathbb{D}^t_{scsp,i,n} = C_i^{t-1} \otimes DO^t_{i,n} \tag{5}$$

It should be noted that the discounted opinions calculated by the SCSP are considered to be independent.

3) The discounted opinion values are then, combined by the SCSP using the consensus operator to obtain the CO set for each node n, which is calculated as follows[1]:

$$C_n^t \quad = \mathbb{D}^t_{scsp,i,n} \oplus \cdots \oplus \mathbb{D}^t_{scsp,j,n} \tag{6}$$

where $C_n^t = (b^t_{scsp,n}, d^t_{scsp,n}, u^t_{scsp,n}, a^t_{scsp,n})$ and nodes $\{i, \cdots, j\}$ refer to those nodes in the system which do not belong to sensor-owner as node n.

4) Finally, the CO set[1], $CO_l^t = (B_l^t, D_l^t, U_l^t, A_l^t)$, for each sensor-owner s_l is calculated by SCSP as the average of C_n^t values of all nodes belonging to the sensor-owner s_l.

With the help of these trust values, DETER enforces trust among oligopolistic sensor-owners in sensor cloud using a game-theoretic dynamic pricing scheme, which is discussed in the following subsection.

4.2 Game-Theoretic Dynamic Pricing Scheme

In this work, we model the interaction between the SCSP and a few registered sensor-owners in service-oriented sensor-cloud using a *Single Leader Multiple Follower Stackelberg* game. Here, we consider that the SCSP acts as the leader, and decides the price to be paid to each sensor-owner, while ensuring QoS of the network and maximizing its own profit. On the other hand, the sensor-owners act as the followers, and provide the service as requested by the SCSP, while ensuring high revenue. The justification for using Stackelberg game theory in this work is discussed as follows.

4.2.1 Stackelberg Game: The Justification:

Game theory is a mathematical tool used to study the complexities of decision making for individuals in competitive scenarios, where each individual influences the other individuals. As mentioned in Section 1, in the SOA of sensor-cloud, there exists an oligopolistic market scenario among a few non-cooperative sensor-owners, where each sensor-owner competes with the other sensor-owners to earn higher profits. Thus, some of the sensor-owners may adopt unfair means to degrade the market reputation of others. These interactions among the sensor-owners, and the sensor-owners and the SCSP are modeled using game theoretic approach. Furthermore, since sensor-cloud has a SOA, it is highly essential that the quality of Se-aaS provided by the SCSP is compliant with the QoS specified in the SLA. Hence, in order to ensure the specified QoS, the SCSP needs to adopt measures for preventing the competitive oligopolistic market situation among the sensor-owners. Therefore, we use a Single-Leader-Multiple-Follower Stackelberg Game in the proposed scheme, DETER. In DETER, the SCSP acts as the leader and takes the pricing decision, while the sensor-owners act as followers and take the decision to behave honestly or dishonestly in the service-oriented sensor-cloud.

4.2.2 Game Formulation

In DETER, initially, the end-users request services to the SCSP, as per their requirements. We consider that the end-user provides information about the type of service required, and the tolerable delay, δ. Based on these information, the SCSP decides the price to be charged, which is denoted by $\mathcal{P}_{max}$. The price $\mathcal{P}_{max}$ is fixed for specific service as per the agreement between the SCSP and the end-user. In the following sections, we discuss the utility functions of the proposed Stackelberg game along with the equilibrium conditions and the solution of the game.

Utility Function for Next-Hop Selection

On receiving the service specifications from the end-users, the SCSP selects the source sensor nodes for delivering the requested services. Each source node needs to forward the generated information to the SCSP within the maximum tolerable delay specified by the end-user. Since, in sensor-cloud, multi-hop communication is used for forwarding data to the BS, the source sensor nodes take help of the intermediate sensor nodes, which may belong to any sensor-owner. In order to select the optimum trustworthy hop nodes for data transmission, each node n calculates a utility function, $\mathcal{U}^t_{n,i}(\cdot)$, for each neighbor node i at time instant t and tries to maximize its payoff.

Motivated by the work of Chatterjee *et al.* [2], we consider that each sensor node n calculates payoff of $\mathcal{U}^t_{n,i}(\cdot)$ for the neighbor nodes at each step, and decides the candidate set of potential data forwarding nodes, $\mathcal{M}^t_n$. The different parameters of $\mathcal{U}^t_{n,i}(\cdot)$ are discussed as follows:

Residual Energy Factor ($\rho^t_{n,i}$)[1]: We define the residual energy factor of node i at time instant t, $\rho^t_{n,i}$, as the ratio of the residual energy of node i at time instant t, $E^t_{res,i}$, and its initial energy, $E_{init,i}$. Hence, we have,

1. For detailed calculation, refer to supplementary file.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

$\mathcal{U}^t_{n,i}(\cdot) > \mathcal{U}^t_{n,j}(\cdot)$ and $i \succ j$, where $(\rho^t_{n,i} > \rho^t_{n,i})$, $\{i,j\} \in N_n$, and other parameters are constant.

Received Signal Strength $(RSS^t_{n,i})^2$: We define the received signal strength, $\mathtt{RSS}^t_{n,i}$, using the *Friis' transmission formula* [30], assuming that there is no power loss due to hardware [31]. With the increase in $\mathtt{RSS}^t_{n,i}$, the payoff of $\mathcal{U}^t_{n,i}(\cdot)$ increases.

Signal-to-Noise Ratio $(SNR^t_{n,i})^2$: The signal to noise ratio, $\mathtt{SNR}^t_{n,i}$, is formulated based on the work of Etezadi *et al.* [32]. With the increase in $\mathtt{RSS}^t_{n,i}$, the payoff of $\mathcal{U}^t_{n,i}(\cdot)$ increases.

Distributed Trust Opinion Set $(DO^t_{n,i})$: We get the distributed trust opinion set, $DO^t_{n,i}$, using Equation (4). We consider that $\mathcal{U}^t_{n,i}$ varies proportionally with the *expectation factor*, which is defined in Definition 2.

Definition 2. *Expectation factor, $EF^t_{n,i}$, is the ratio of the trust expectation value, $BE^t_{n,i}$, and the distrust expectation value, $DE^t_{n,i}$. Here, $BE^t_{n,i} = b^t_{n,i} + a^t_{n,i}u^t_{n,i}$, and $DE^t_{n,i} = d^t_{n,i} + (1 - a^t_{n,i})u^t_{n,i}$, and $a^t_{n,i}$ determines the fraction of uncertainty that can contribute as belief.*

By choosing a next-hop node i with high values of the above mentioned factors, the node n ensures that high quality data is provided to the SCSP, i.e., it gains in terms of QoS. We quantify the gain of node n, for selecting node i, in terms of the *virtual revenue function*, $\mathcal{RF}^t_{n,i}(\cdot)$, as follows,

$$\mathcal{RF}^t_{n,i}(\cdot) = \omega_1\rho^t_{n,i} + \omega_2\frac{\mathtt{RSS}^t_{n,i}}{\mathtt{RSS}_{max}} + \omega_3\frac{\mathtt{SNR}^t_{n,i}}{\mathtt{SNR}_{max}} + \omega_4\mathtt{EF}^t_{n,i} \tag{7}$$

where ω_1, ω_2, ω_3 and ω_4 are constants representing the effect of each parameter on the revenue function. $\mathtt{RSS}_{max}$ and $\mathtt{SNR}_{max}$ define the received signal strength and the signal-to-noise ratio at distance d_0, where $0 < d_0 << r_n$, and r_n is the communication range of node n.

Pseudo-Price for Selecting Next-Hop (p^t_i): The price p^t_i to be paid to the selected next-hop node $i \in \mathcal{O}_l$ has a negative impact over $\mathcal{U}^t_{n,i}(\cdot)$, where p^t_i is defined as follows:

$$p^t_i = \Phi\mathtt{TE}^{t^2}_l \tag{8}$$

where Φ is a constant, and $\mathtt{TE}^t_l$ is the trust expectation value for the sensor-owner s_l, where $i \in \mathcal{O}_l$, which is calculated by SCSP and defined as — $\mathtt{TE}^t_l = B^t_l + A^t_l U^t_l$.

Distance from the Base Station $(d_{BS,i})$: The utility function, $\mathcal{U}^t_{n,i}(\cdot)$, varies inversely with the distance between the node i and the BS, $d_{BS,i}$, as selecting a hop node closer to the BS reduces the total number of hops in the path.

Here, both the pseudo-price function as well as the distance from BS of the node i have a negative impact on the payoff from the utility function. Hence, we consider these two factors as the *cost* node n bears for choosing node i as the next-hop and define the *virtual cost function*, $\mathcal{CF}^t_{n,i}(\cdot)$, as follows:

$$\mathcal{CF}^t_{n,i}(\cdot) = \omega_5 p^t_i + \omega_6\frac{d_{BS,i}}{d_{BS,n}} \tag{9}$$

where ω_5 and ω_6 are constants.

Therefore, we define the utility function $\mathcal{U}^t_{n,i}(\cdot)$, of node i evaluated by node n, as the net virtual profit that node n incurs for choosing node i as the next-hop. We have,

$$\mathcal{U}^t_{n,i}(\cdot) = \mathcal{RF}^t_{n,i}(\cdot) - \mathcal{CF}^t_{n,i}(\cdot) \tag{10}$$

Each node n tries to maximizes the payoff of $\mathcal{U}^t_{n,i}(\cdot)$ for choosing optimal candidate set, $\mathcal{M}^t_n$, while satisfying the following constraints along with $\mathtt{RSS}^t_{n,i} \geq \mathtt{RSS}_{th}, \mathtt{SNR}^t_{n,i} \geq \mathtt{SNR}_{th}$:

$$E^t_{res,i} \geq E_{res,th}, d_{BS,i} \leq d_{BS,n} \tag{11}$$

where $E_{res,th}$ and b_{th} indicate the threshold values for residual energy and belief of a node, respectively. $\mathtt{RSS}_{th}$ and $\mathtt{SNR}_{th}$ define the received signal strength and the SNR at distance r_n, where r_n is the communication range of node n. Hence, after calculating the payoff values for each node $i \in N_n$ using Equation (10), the sensor node n decides the candidate set of potential data forwarding nodes, $\mathcal{M}^t_n$, where $|\mathcal{M}^t_n|$ is decided by the SCSP.

Utility Function for Path Selection

The utility function of the SCSP, $\mathcal{P}^t_{path_g}$, is defined as the revenue of the SCSP for selecting path $path_g$, while taking into account the trust value of the chosen path $path_g$. We consider that $\mathbb{N}_{path_g}$ defines the set of sensor nodes belonging to the path $path_g$. Given the maximum tolerable delay, δ, the following constraint needs to be satisfied for each service:

$$|\mathbb{N}_{path_g}| \leq (\delta + 1) \tag{12}$$

We consider that unit delay is incurred at each hop, and there are $|\mathbb{N}_{path_g} - 2|$ number of intermediate sensor nodes. When the control packets forwarded by the source sensor nodes reach the BS through multiple paths, the SCSP calculates the payoff of the utility function for each path $path_g$, and selects the path having the maximum payoff. We consider that the price $\mathcal{P}_{max}$, to be paid by the end-users, includes the profit of the SCSP with two types of cost — hardware cost, $\mathcal{P}_{hw}$, and infrastructure cost, $\mathcal{P}_{infra}$ [2], i.e., $\mathcal{P}_{max} = \mathcal{P}_{hw} + \mathcal{P}_{infra} + \varphi$. We consider that $\mathcal{P}_{infra}$ is directly proportional to the number of virtual sensors used for a service, and the duration of service. For a particular virtual sensor, the price to be paid is constant for unit time. On the other hand, the revenue of the SCSP, φ, varies based on the trust factor of the selected sensor-owners. In order to ensure non-negative profit of the SCSP, we need to ensure $\varphi > 0$. $\mathcal{P}_{hw}$ depends on the cost incurred due to the use of sensor nodes for providing a particular service, and

2. For detailed calculation, refer to supplementary file.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

$\mathcal{P}_{hw} = \mathcal{P}^s_{hw} + \mathcal{P}^r_{hw}$. $\mathcal{P}^s_{hw}$ and $\mathcal{P}^r_{hw}$ are the costs incurred for sensing and relaying, respectively. $\mathcal{P}^s_{hw}$ is only paid to the source nodes, which generate the sensor data. $\mathcal{P}^r_{hw} = \sum_{\forall n} P_n$, and $n \in path_g$. P_n defines the price to be paid to each sensor node n, which are in path $path_g$. We assume that P_n for sensor node n varies proportionally with the normalized pseudo price, $\mathtt{TE}^t_k$, of the sensor-owner k, where $n \in \mathcal{O}_k$. Hence, we get:

$$P_n = \chi[{\mathtt{TE}^t_k}^2 / \sum_{n \in path_g} \{{\mathtt{TE}^t_k}^2 | n \in \mathcal{O}_k\}] \quad (13)$$

where χ is a constant and defines the price for fully trusted sensor-owner s_k, i.e., $CO^t_k = (1, 0, 0, A^t_k)$. Hence, for provisioning service within the specified delay and ensuring high profit, the SCSP tries to maximize the payoff of the utility function, $\mathcal{P}^t_{path_g}$, defined as below:

$$\mathcal{P}^t_{path_g} = 1 - \frac{\mathcal{P}_{hw}}{\mathcal{P}_{max}} + \prod_{k, n \in \mathcal{O}_k}^{n \in path_g} \frac{B^t_k + A^t_k U^t_k}{D^t_k + (1 - A^t_k) U^t_k} \quad (14)$$

To account for the cumulative effect of the trust opinion set of each node in path $path_g$, we introduce the product function in Equation (14).

4.2.3 Existence of Stackelberg Equilibrium

As discussed in Section 4.2.2, in DETER, the selection of the next-hop node i by node n not only depends on the physical parameters of node i, but also depends on the distributed trust opinion of node n for node i and the centralized trust opinion of SCSP for the owner of node i. Additionally, the price to be paid by the SCSP to node n depends on the action taken by node n, i.e., the next hop selected by node n, and the centralized trust opinion for owner of node n. Thereby, there exists a non-cooperative game among the competitive sensor-owners, in which each sensor-owner tries to maximize his/her revenue by increasing the chances of selection of his/her sensor nodes as well as by selecting the optimum next-hop node for data forwarding.

Given the values of the centralized trust opinion sets calculated by the SCSP, the optimal response, known as the *reaction set* of the sensor nodes, is determined as the set of *Nash Equilibrium* strategies for the sensor nodes. Here, Nash Equilibrium refers to the equilibrium state of the followers at which none of the players, i.e., sensor owner, gain benefit by unilaterally deviating from the chosen strategy [33] On obtaining the reaction set of the sensor nodes, the SCSP decides the optimum strategy, i.e., the path for data-transmission, having maximum payoff value, which is known as *Stackelberg Equilibrium* [34]. In other words, Stackelberg Equilibrium refers to the equilibrium state of the system having leader-follower hierarchy at which the leader chooses the strategy which yields the maximum pay-off given the set of Nash Equilibrium strategy of the followers. Hence, we define the Stackelberg equilibrium for the non-cooperative oligopolistic market of sensor-cloud as in Definition 3. Additionally, the existence of Nash equilibrium is shown in Theorem 1. For the distributed equilibrium solution of DETER, the reader is requested to refer to the supplementary file.

Definition 3. *The Stackelberg equilibrium of DETER is defined as $(b^{t*}_{n,i}, d^{t*}_{n,i}, B^{t*}_l, D^{t*}_l)$, where the proposed scheme ensures the following conditions are satisfied:*

$$\mathcal{U}^t_{n,i}(b^{t*}_{n,i}, d^{t*}_{n,i}, B^t_l, D^t_l) \geq \mathcal{U}^t_{n,i}(b^t_{n,i}, d^t_{n,i}, B^t_l, D^t_l) \text{ and } \mathcal{P}^t_{path_g}(b^{t*}_{n,i}, d^{t*}_{n,i}, B^{t*}_l, D^{t*}_l) \geq \mathcal{P}^t_{path_g}(b^{t*}_{n,i}, d^{t*}_{n,i}, B^t_l, , D^t_l) \quad (15)$$

where $b^{t*}_{n,i}, d^{t*}_{n,i}$ are the optimum belief and disbelief values of the chosen node $i \in N_n$ by node n, and B^{t*}_l, D^{t*}_l are the optimum belief and disbelief values of sensor-owner l, where $i \in \mathcal{O}_l$.

Theorem 1. *Given the set of neighbor nodes N_n of node n, and the price function, which varies polynomially with the trust expectation value $\mathtt{TE}^t_l$, where $\forall i \in (N_n \cap \mathcal{O}_l)$, there exists Nash equilibrium, if we have negative values for variational inequality of $\mathcal{U}^t_{n,i}(\cdot)$ with respect to $b^t_{n,i}$, and positive values for variational inequality of $\mathcal{U}^t_{n,i}(\cdot)$ with respect to $d^t_{n,i}$.*

Proof: For the proof of Theorem 1, refer to supplementary file. □

Lemma 1. *From Theorem 1, we conclude that DETER ensures the existence of Stackelberg Equilibrium, as there exists Nash Equilibrium among the followers. The Stackelberg Equilibrium can be obtained by selecting the path which maximizes the payoff of the utility function $\mathcal{P}^t_{path_g}$ of the SCSP.*

5 Proposed Algorithms

The detailed working of the proposed scheme DETER is presented using an interaction diagram in Figure 3. In DETER, each sensor node n calculates DO set for its neighbor nodes, $\mathcal{N}_n$, periodically, using Algorithm 1. Based on DO calculated by the sensor nodes, $\mathcal{N}$, the SCSP calculates the CO for the registered sensor-owners, $\mathcal{S}$, using Algorithm 2. In sensor-cloud, the source nodes needs to establish a path to BS, in order to transmit sensed data to the SCSP. Hence, the source node and the selected intermediate nodes execute Algorithm 3 to determine the candidate set for next-hop node selection. Thereafter, the SCSP performs an optimization algorithm, i.e., Algorithm 4, for selecting the path having optimum cumulative trust values to provide high quality service. Using Algorithm 4, the SCSP also ensures its own profit and the profit of the sensor-owners based on the their centralized trust opinion sets. The detailed pseudo-codes of the Algorithms 1-4 are given in the supplementary file.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

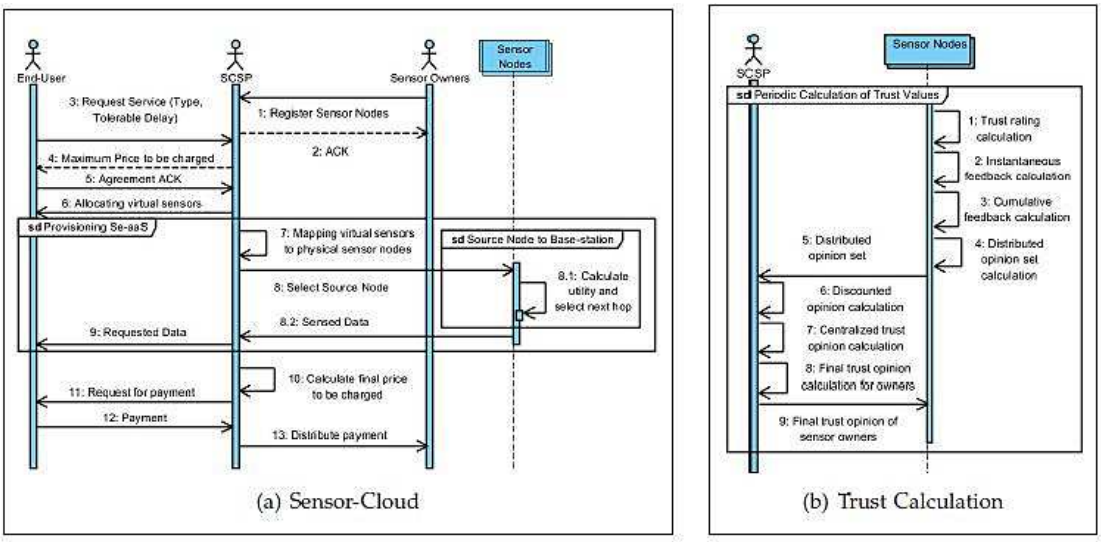

Fig. 3: Interaction Diagram of DETER

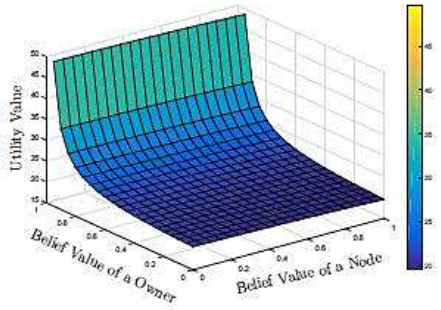

Fig. 4: Theoretical Analysis of Utility value

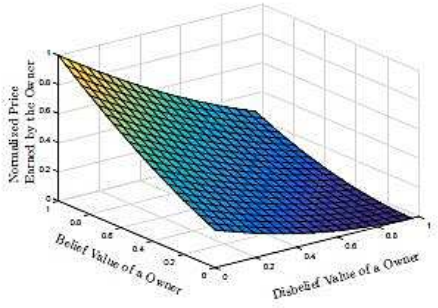

Fig. 5: Price with Varying Trust of Sensor-Owners

6 Performance Evaluation

6.1 Simulation Parameters

To evaluate the performance of the proposed scheme, DETER, we consider that the heterogeneous sensor nodes, i.e., having different types of sensors, are deployed over the terrain in a random pattern, and the BS is at the center of the terrain, in a MATLAB simulation platform. Additionally, we consider that the heterogeneous sensor nodes use the IEEE 802.15.4 protocol for communication, as shown in Table 2. Hence, the size of `Hello` packet is 6 *bytes*, and each `Data` packet has a payload of 128 *bytes*. For simulation purpose, we have selected the source node randomly based on the available sensors and the application requirements of the end-users. Initially, we consider that each node sends 100 packets to its neighbor nodes for calculating the distributed trust opinion sets. Thereafter, based on the request of the SCSP, the sensor nodes send packets to the BS. Additionally, we assume that for each service of one hour, 180 packets are sent to the SCSP, as shown in Table 2.

TABLE 2: Simulation Parameters

Parameter	Value
Simulation area	1000 m×1000 m
Number of sensor nodes	$400 - 800$
Number of sensor owners	4
Type of sensor nodes	3
$\lvert\mathcal{M}_n^t\rvert$	$3 - 5$
Number of BS	1
Communication protocol	IEEE 802.15.4
Initial energy of each node	20 J [31]
Communication range	100 m
Packet Header size	6 $bytes$
Packet Payload size	128 $bytes$
Packet transmission rate	180 $packets/hr/service$
Tx energy consumption	50 nJ/bit [35]
Rx energy consumption	50 nJ/bit [35]
Energy consumption at amplifier	100 $pJ/bit\text{-}m^2$ [35]

6.2 Benchmarks

We compared the proposed scheme, DETER, with two different existing schemes — dynamic optimal pricing for heterogeneous services-oriented architecture (referred in this paper as DOP) [2] and trust and energy aware routing protocol (TERP) [21]. In DOP [2], Chatterjee *et al.* proposed a pricing scheme for hardware resource usage in sensor-cloud. The authors proposed that path selection is done at the beginning of each service based on physical parameters of nodes. The price charged by the owners of the selected nodes

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

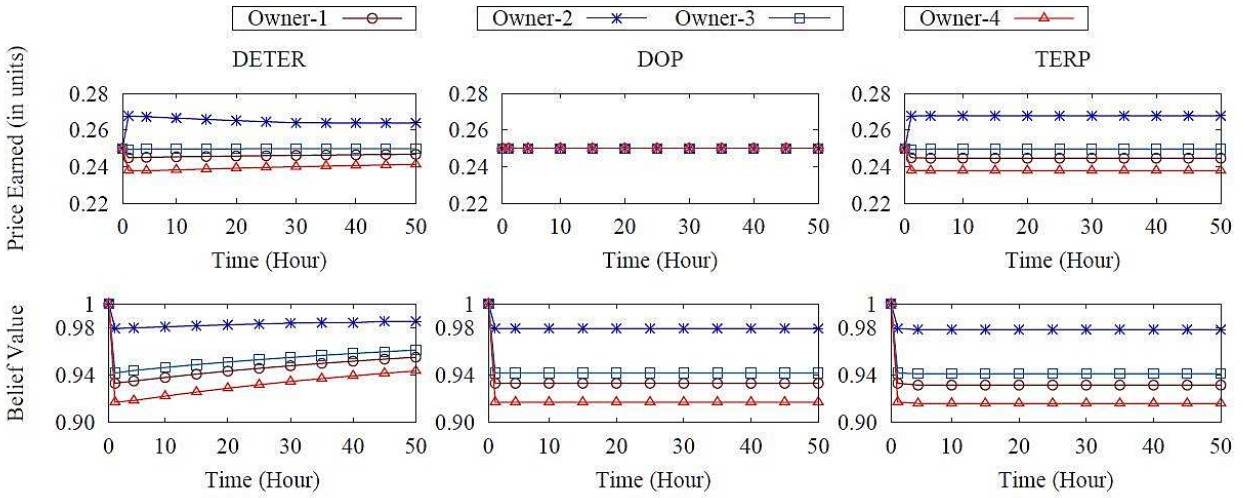

Fig. 6: Comparitive Analysis of Belief Value and Price Earned by Sensor-Owners

is determined from the price charged by the previous hop and the estimated price to be paid by the end-user. However, the selfish behavior of the sensor-owners is not considered in DOP. Hence, trust of the selected path is not ensured. On the other hand, in TERP, Ahmed *et al.* [21] studied a routing scheme to eliminate misbehaving or faulty nodes from path. Trust rating of each node is determined based on its opinion about itself as well as the opinions of its neighbor nodes. However, this approach cannot be used in sensor-cloud, as the presence of multiple sensor-owners and the economic aspect of the sensor-cloud, i.e., the profits of the SCSP and the sensor-owners, are not considered. Using the proposed scheme, DETER, we can ensure QoS of Se-aaS with high trust values in presence of multiple sensor-owners and high profits, than using DOP and TERP.

6.3 Performance Metrics

We evaluated the performance of the proposed scheme, DETER, using the following metrics.

Explored Nodes: To provide a particular service for an hour, the value of explored nodes is calculated as the average of the total number of nodes explored in the network, before finalizing the path, from the chosen source node to the BS. With the increase in the number of explored nodes in the network, the system performance deteriorates.

Total and Correctly Forwarded Packets: We calculate the network overhead by analyzing the total number of data packets sent by the nodes. For evaluation, we considered the average number of packets forwarded by the nodes in an hour as the *total forwarded packets*, `totPackets`. Additionally, the *percentage of correctly forwarded packets*, `percentCorPackets`, varies linearly with the ratio of the number of packets forwarded correctly, `corPackets`, to the total number of packets forwarded.

Average Path Length: The average number of nodes in the path selected for each hour of service is termed as the *average path length*, $\mathbb{N}_{path_g}$. Hence, the average number of hops in each path is given by, $(\mathbb{N}_{path_g} - 1)$.

Average Number of Selfish Nodes in Path: We consider a node as selfish, if it belongs to a selfish sensor-owner. With the increase in the number of selfish nodes in a path, the QoS provided by the SCSP to the end-user decreases.

Network Lifetime: We define network lifetime as the time elapsed after node deployment till when the last node dies in the network. For better performance of the network, we need to ensure high network lifetime.

Price paid by SCSP to sensor-owners: The profits of the sensor-owner increases linearly with the increase in the price paid to them by the SCSP. Each sensor-owner $s_l \in \mathcal{S}$ gets paid, if and only if, any node i belonging to the sensor-owner, i.e., $i \in \mathcal{O}_l$, is present in the selected path, $path_g$.

Profit of SCSP: The profit of the SCSP is defined as the difference between the amount received by the SCSP from the end-users in exchange of the provided service and the amount spent by the SCSP for provisioning the service, which includes the price paid to the sensor-owners and the cost incurred for providing infrastructural resources.

6.4 Results and Discussions

We observe that, in DETER, with the increase in belief value of each sensor-owner s_l, the utility value of each node $n \in \mathcal{O}_l$ varies almost exponentially, considering that the belief of node n is fixed, as shown in Figure 4. On the other hand, with the increase in the belief value of each sensor node $n \in \mathcal{O}_l$, the utility value of the node varies insignificantly with the belief value of the sensor-owner remaining fixed. This is because in DETER, the next hop node selection is highly dependent on the belief value of the sensor-owners, in order to resist monopoly situation. In Figure 5,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

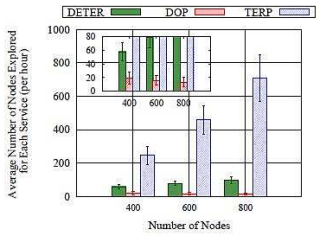

Fig. 7: Number of Nodes Explored

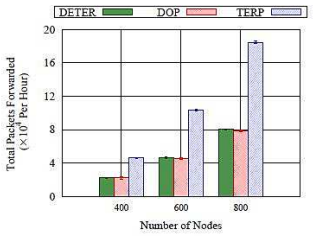

Fig. 8: Network Overhead

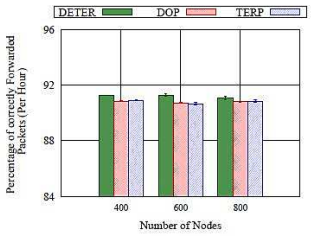

Fig. 9: Correctly Forwarded Packet

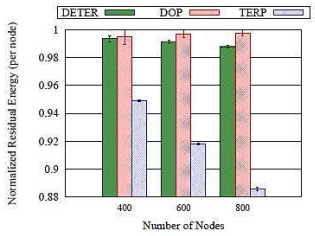

Fig. 10: Residual Energy of Nodes

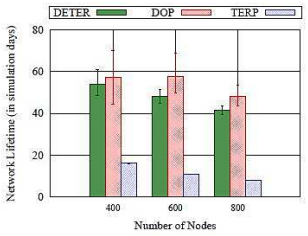

Fig. 11: Network lifetime

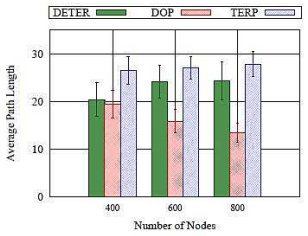

Fig. 12: Average Path Length

we observe that for fixed belief value, the price paid by the SCSP to a sensor-owner decreases with the increase in his/her disbelief value. With the increase in belief value and decrease in disbelief value of the sensor-owner, s/he earns higher price from SCSP.

Moreover, a comparative analysis of DETER, DOP and TERP is shown in Figure 6. We observe that the belief value of each sensor-owner increases with time using DETER, whereas for DOP and TERP, it remains constant with time. This is due to the fact that DETER encourages each sensor-owner to behave honestly by paying less price as shown in Figure 6. Additionally, we observe that the price earned by each sensor-owner increases with the increase in individual belief value. However, in DOP, the sensor owners earn the same price irrespective of their belief values, as DOP does not consider trust value for price calculation. In case of TERP, the price earned by each sensor-owner depends on his/her belief value. As the belief values remain fixed, the price earned by the sensor-owners remain unchanged.

Figures 7, 8, and 9 depict that DETER outperforms the existing schemes — DOP and TERP. Though the average number of nodes explored in DETER is higher than that in DOP, DETER explores 76.57-86.47% less number of nodes than TERP. In the path exploration phase, unlike DOP, DETER and TERP explore multiple paths from each source node to the BS. The SCSP finalizes the path to be used for data forwarding from the multiple choices of paths. However, DOP depends on single path exploration for each source-BS pair. Moreover, DETER and TERP are capable of facilitating the change of path, if any faulty or misbehaving node is detected in the path. We also get that the network overhead decreases by 52.6-56.53% using DETER, than using TERP. Additionally, using DETER, the percentage of correctly forwarded packets increases by 0.23-0.62% and 0.27-0.56% than using DOP and TERP, respectively. Additionally, we observed that in sensor-cloud, TERP does not always guarantee a path between the source node and the BS, as in TERP, each node only chooses the next-hop nodes which have trust value greater than 0.6 [21].

Using DETER, the residual energy of each node is almost similar to that using DOP, and 4.69-11.56% higher than that of TERP, as depicted in Figure 10. This is due to the fact that, using DOP, the energy consumed for node exploration is less than using DETER and TERP. Therefore, we conclude that DETER ensures trust-based QoS in sensor-cloud without consuming high amount of energy. The claim is also supported by the Figure 11. From Figure 11, we observe that the network lifetime is higher using DOP than using DETER, as using DOP, the number of nodes explored increases linearly with the increase in hop count. Whereas, using DETER and TERP, the the number of nodes explored increases exponentially with the increase in hop count. In DETER, owing to the restriction in the cardinality of the candidate set, the number of nodes explored is bounded. However, using TERP, the available nodes having trust rating greater than or equal to 0.6 are explored. Therefore, using TERP, the energy consumption of the network is higher than using DETER. Hence, we observe that there is a significant increase in the network lifetime by using DETER as compared to TERP.

In Figure 12, we observe that for a service, the average length of the final path obtained using DETER improves by 10.87-23.21% than using TERP. Using TERP, the average path length is higher than DETER due to the fact that in TERP, the intermediate nodes in a path must have trust values greater than 0.6 [21], as mentioned earlier. In DOP, neighbor nodes which are closer to the BS are given higher preference. Hence, with the increase in number of total deployed nodes, the average path length shows a decreasing

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

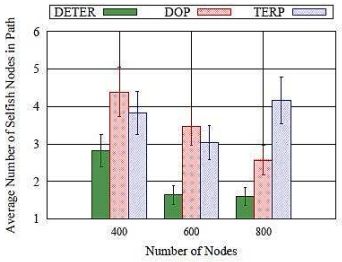

Fig. 13: Selfish Nodes in a Path

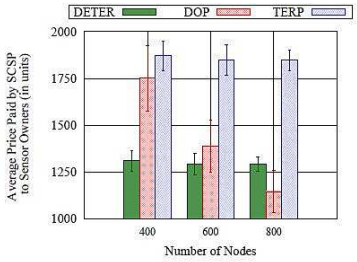

Fig. 14: Price Paid by SCSP

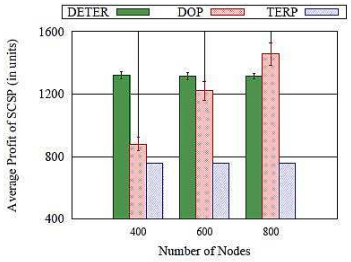

Fig. 15: Profit of the SCSP

trend. However, since trust value of the nodes is not considered, DOP fails to ensure trust of the path. On the other hand, using DETER, the number of selfish nodes in the path is reduced by 35.61-52.72% and 26.43-61.37% than using DOP and TERP, respectively, as shown in Figure 13.

Figures 14 and 15 imply that using DETER, the amount earned by the sensor-owners and the profit of the SCSP is almost similar with the increase in the number of nodes. However, using the existing schemes — DOP and TERP, high profit of the sensor-owners and the SCSP cannot be ensured at the same time, in sensor-cloud. From Figure 14, we note that the price to be paid by the SCSP to the sensor-owners decreases by at most 25.2% and 30% by using DETER, than using DOP and TERP, respectively. Correspondingly, we observe that the profit of the SCSP increase by at most 50.15% and 73.9% using DETER than by using DOP and TERP, respectively. We obtain these results due to the fact that unlike DETER, the SCSP does not penalize the selfish sensor owners in DOP. Thus, using DOP, the profit of the SCSP reduces than using DETER. Therefore, we conclude that in DETER, we ensure trust in the presence of multiple sensor-owners in sensor-cloud by using the proposed dynamic pricing scheme. Moreover, DETER yields high network lifetime, while ensuring high QoS in sensor-cloud as compared to the existing schemes.

7 Conclusion

In this paper, we formulated a Single-Leader-Multiple-Follower Stackelberg game theory-based dynamic pricing scheme for sensor-cloud in order to enforce trust among the oligopolistic sensor-owners. In DETER, each sensor node calculates distributed trust opinion set for its neighbor nodes, locally. Based on the distributed trust opinion sets, the SCSP determines the centralized trust opinion set for each registered sensor-owner. The sensor nodes use these trust opinion sets to select their next-hop nodes. On the other hand, the SCSP decides the price to be paid to each sensor-owner based on the centralized trust opinion set. From simulation, we observe that using DETER, network lifetime and the percentage of correctly forwarded packets increases. Moreover, the number of selfish nodes in the path decreases using DETER which compels the sensor-owners to behave honestly. Additionally, DETER ensures high profits of both the sensor-owners and the SCSP.

This work can be extended to ensure high QoS of Se-aaS provided by the SCSP in the presence of unintentional failures of the sensor nodes in sensor-cloud. Additionally, the influence of external attackers in sensor-cloud can also be explored. It can also be extended to understand service provisioning mechanism for mobile sensor-cloud in presence of multiple sensor-owners.

References

[1] S. Misra, S. Chatterjee, and M. S. Obaidat, "On Theoretical Modeling of Sensor Cloud: A Paradigm Shift From Wireless Sensor Network," *IEEE Syst. J.*, vol. 11, no. 2, pp. 1084–1093, Jun 2017.

[2] S. Chatterjee, R. Ladia, and S. Misra, "Dynamic Optimal Pricing for Heterogeneous Service-Oriented Architecture of Sensor-cloud Infrastructure," *IEEE Trans. on Serv. Comp.*, vol. 10, no. 2, pp. 203–216, Mar 2017.

[3] P. Chavali and A. Nehorai, "Managing Multi-Modal Sensor Networks Using Price Theory," *IEEE Trans. on Sig. Proc.*, vol. 60, no. 9, pp. 4874–4887, Sept 2012.

[4] L. Guijarro, V. Pla, J. R. Vidal, and M. Naldi, "Maximum-Profit Two-Sided Pricing in Service Platforms Based on Wireless Sensor Networks," *IEEE Wireless Comm. Let.*, vol. 5, no. 1, pp. 8–11, Feb 2016.

[5] K. W. Park, J. Han, J. Chung, and K. H. Park, "THEMIS: A Mutually Verifiable Billing System for the Cloud Computing Environment," *IEEE Trans. on Serv. Comp.*, vol. 6, no. 3, pp. 300–313, Jul 2013.

[6] S. Chaisiri, B. S. Lee, and D. Niyato, "Optimization of Resource Provisioning Cost in Cloud Computing," *IEEE Trans. on Serv. Comp.*, vol. 5, no. 2, pp. 164–177, Apr 2012.

[7] A. Jøsang and R. Ismail, "The Beta Reputation System," in *Proc. of the* 15^{th} *Bled Elect. Com. Conf.*, vol. 5, 2002, pp. 2502–2511.

[8] K. Ahmed and M. Gregory, "Integrating Wireless Sensor Networks with Cloud Computing," in *Proc. of the* 7^{th} *Int. Conf. on Mobile Ad-hoc and Sens. Net.*, Dec 2011, pp. 364–366.

[9] M. Yuriyama and T. Kushida, "Sensor-Cloud Infrastructure - Physical Sensor Management with Virtualized Sensors on Cloud Computing," in *Proc. of the* 13^{th} *Int. Conf. on Net.-Based Inform. Syst.*, Sept 2010, pp. 1–8.

[10] S. Bose, N. Mukherjee, and S. Mistry, "Environment Monitoring in Smart Cities Using Virtual Sensors," in *Proc. of the* 4^{th} *IEEE Int. Conf. on Future Int. of Things and Cloud*, Aug 2016, pp. 399–404.

[11] S. Madria, V. Kumar, and R. Dalvi, "Sensor Cloud: A Cloud of Virtual Sensors," *IEEE Softw.*, vol. 31, no. 2, pp. 70–77, Mar 2014.

[12] S. Chatterjee and S. Misra, "Optimal Composition of a Virtual Sensor for Efficient Virtualization within Sensor-Cloud," in *Proc. of IEEE Int. Conf. on Comm.*, Jun 2015, pp. 448–453.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSC.2018.2873763, IEEE Transactions on Services Computing

[13] S. Chatterjee and S. Misra, "Dynamic and Adaptive Data Caching Mechanism for Virtualization within Sensor-Cloud," in *Proc. of IEEE Adv. Net. and Tel. Syst.*, Dec 2014, pp. 1–6.

[14] S. Chatterjee, S. Misra, and S. Khan, "Optimal Data Center Scheduling for Quality of Service Management in Sensor-Cloud," *IEEE Trans. on Cloud Comp.*, 2015, DOI: 10.1109/TCC.2015.2487973.

[15] T. Ojha, S. Bera, S. Misra, and N. S. Raghuwanshi, "Dynamic Duty Scheduling for Green Sensor-Cloud Applications," in *Proc. of the IEEE* 6^{th} *Int. Conf. on Cloud Comp. Tech. and Sci.*, Dec 2014, pp. 841–846.

[16] S. Misra, S. Bera, A. Mondal, R. Tirkey, H. C. Chao, and S. Chattopadhyay, "Optimal Gateway Selection in Sensor-Cloud Framework for Health Monitoring," *IET Wireless Sens. Syst.*, vol. 4, no. 2, pp. 61–68, Jun 2014.

[17] S. Chatterjee, S. Sarkar, and S. Misra, "Energy-Efficient Data Transmission in Sensor-Cloud," in *Proc. of App. and Innov. in Mobile Comp.*, Feb 2015, pp. 68–73.

[18] V. P. Illiano and E. C. Lupu, "Detecting Malicious Data Injections in Wireless Sensor Networks: A Survey," *ACM Comp. Surv.*, vol. 48, no. 2, pp. 24:1–24:33, 2015.

[19] X. Li, F. Zhou, and J. Du, "LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks," *IEEE Trans. on Inform. Foren. and Sec.*, vol. 8, no. 6, pp. 924–935, Jun 2013.

[20] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks," *IEEE Trans. on Dep. and Sec. Comp.*, vol. 12, no. 1, pp. 98–110, Jan 2015.

[21] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network," *IEEE Sen. J.*, vol. 15, no. 12, pp. 6962–6972, Dec 2015.

[22] H. Rathore, V. Badarla, and S. Shit, "Consensus-Aware Sociopsychological Trust Model for Wireless Sensor Networks," *ACM Trans. on Sens. Net.*, vol. 12, no. 3, pp. 21:1–21:27, Aug 2016.

[23] D. Ardagna, B. Panicucci, and M. Passacantando, "Generalized Nash Equilibria for the Service Provisioning Problem in Cloud Systems," *IEEE Trans. on Serv. Comp.*, vol. 6, no. 4, pp. 429–442, Oct 2013.

[24] D. Ardagna, M. Ciavotta, and M. Passacantando, "Generalized Nash Equilibria for the Service Provisioning Problem in Multi-Cloud Systems," *IEEE Trans. on Serv. Comp.*, vol. 10, no. 3, pp. 381–395, May 2017.

[25] S. Buchegger and J.-Y. Boudec, "Performance Analysis of the CONFIDANT Protocol," in *Proc. of ACM Int. Symp. on Mobile Ad-Hoc Net. & Comp.*, New York, USA, 2002, pp. 226–236.

[26] U. B. I. Maarouf and A. R. Naseer, "Efficient Monitoring Approach for Reputation System-Based Trust-Aware Routing in Wireless Sensor Networks," *IET Comm.*, vol. 3, no. 5, pp. 846–858, May 2009.

[27] A. Jøsang, "A Logic for Uncertain Probabilities," *Int. J. of Uncert., Fuzz. and Know.-Based Syst.*, vol. 9, no. 3, pp. 279–311, Jun 2001.

[28] A. Jøsang, "The Consensus Operator for Combining Beliefs," *Artificial Intell.*, vol. 141, no. 1, pp. 157–170, Oct 2002.

[29] Y. Sun, H. Luo, and S. K. Das, "A Trust-Based Framework for Fault-Tolerant Data Aggregation in Wireless Multimedia Sensor Networks," *IEEE Trans. on Dep. and Sec. Comp.*, vol. 9, no. 6, pp. 785–797, Nov 2012.

[30] H. T. Friis, "A Note on a Simple Transmission Formula," *Proc. of the IRE*, vol. 34, no. 5, pp. 254–256, May 1946.

[31] S. Misra, G. Mali, and A. Mondal, "Distributed Topology Management for Wireless Multimedia Sensor Networks: Exploiting Connectivity and Cooperation," *Int. J. of Comm. Syst.*, vol. 28, no. 7, pp. 1367–1386, May 2015.

[32] F. Etezadi, K. Zarifi, A. Ghrayeb, and S. Affes, "Decentralized Relay Selection Schemes in Uniformly Distributed Wireless Sensor Networks," *IEEE Trans. on Wireless Comm.*, vol. 11, no. 3, pp. 938–951, Mar 2012.

[33] Z. Han, D. Niyato, W. Saad, T. Basar, and A. Hjorungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*, 1st ed. New York, NY, USA: Cam. Univ. Press, 2012.

[34] A. Mondal, S. Misra, and M. S. Obaidat, "Distributed Home Energy Management System With Storage in Smart Grid Using Game Theory," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1857–1866, September 2017.

Aishwariya Chakraborty (S'17) is presently a pursuing her M.S. degree from Dept. of Computer Science and Engineering, IIT Kharagpur, India. Her current research interests include algorithm design for sensor-cloud, service-oriented architecture, and wireless sensor networks. She received her B.Tech. degree from West Bengal University of Technology in 2015. She is a student member of IEEE.

Ayan Mondal (S'13) is presently a TCS Fellow and pursuing his Ph.D. degree from Dept. of CSE, IIT Kharagpur, India. His current research interests include algorithm design for smart grid and wireless sensor networks. He received his M.S. and B.Tech. degree from IIT Kharagpur in 2014 and West Bengal University of Technology in 2012, respectively. He is a student member of IEEE and ACM.

Arijit Roy (S'13) is presently a CSIR Fellow and pursuing his Ph.D. degree from Advanced Technology Development Centre, IIT Kharagpur, India. His research interests include mobile ad-hoc networks and wireless sensor networks. He received his M.S. and B.Tech. degree from IIT Kharagpur and West Bengal University of Technology, respectively. He is a student member of IEEE.

Sudip Misra (SM'11) is a Professor at the IIT Kharagpur. He received his Ph.D. degree from Carleton University, Ottawa, Canada. Dr. Misra is the author of over 300 scholarly research papers. He has won several national and international awards including the IEEE ComSoc Asia Pacific Young Researcher Award during IEEE GLOBECOM 2012. Dr. He was also the recipient of several academic awards and fellowships such as the NASI Fellow Award (National Academy of Sciences, India), the Young Scientist Award (National Academy of Sciences, India), Young Systems Scientist Award (Systems Society of India), and Young Engineers Award (Institution of Engineers, India). Misra was also invited to deliver keynote/invited lectures in over 30 international conferences in USA, Canada, Europe, Asia and Africa.