Trust-Based Communication for the Industrial Internet of Things

Chunsheng Zhu, Joel J. P. C. Rodrigues, Victor C. M. Leung, Lei Shu, and Laurence T. Yang

Studying the performance of IIoT, the authors investigate trust-based communication for IIoT. In particular, devoting attention to sensor-cloud, which is a paradigm of IIoT, they propose three types of trust-based communication mechanisms for sensor-cloud. Furthermore, with numerical results, they show that trust-based communication can greatly enhance the performance of sensor-cloud.

Abstract

Recently, the Industrial Internet of Things (IIoT) is attracting growing attention from both academia and industry. Meanwhile, trust-based communication is widely utilized in various systems. In this article, studying the performance of IIoT, we investigate trust-based communication for IIoT. In particular, devoting attention to sensor-cloud, which is a paradigm of IIoT, we propose three types of trust-based communication mechanisms for sensor-cloud. Furthermore, with numerical results, we show that trust-based communication can greatly enhance the performance of sensor-cloud. Eventually, open research issues with respect to trust-based communication for sensor-cloud are discussed.

Introduction

Lately, with a number of interesting applications (e.g., industrial equipment monitoring, industrial property management, smart manufacturing, smart factory), the Industrial Internet of Things (IIoT) is attracting increasing attention from both academia and industry. Particularly, IIoT [1] is an internet in which everything in industry is connected and interacts with each other. By integrating the physical objects, cyber objects, and social objects in industry, IIoT has the purpose of behaving intelligently to better serve people in industry. For instance, smart surveillance systems [2] could be enabled for petrochemical plants with IIoT by converging cyber-physical systems and social spaces.

In the meantime, as a performance enhancement mechanism, trust-based communication [3] is widely used in various systems (e.g., social-based systems, network-based systems, computer-based systems). Specifically, defined by Merriam-Webster, trust is the "assured reliance on the character, ability, strength, or truth of someone or something." By incorporating trust (e.g., trust value, trust value threshold) into communication, trust-based communication performs communication on the basis of entities (e.g., individual, network node, server) that can be trusted, with the aim of enhancing the quality of service (QoS) of the system. For example, the security and energy efficiency for a wireless network system can be improved [4] by obtaining network node trust with a number of detection routes.

In this article, exploring the performance of IIoT, we investigate trust-based communication for IIoT. In particular, focusing on sensor-cloud [5], which is a paradigm of IIoT, we introduce three types of trust-based communication mechanisms for sensor-cloud. In addition, with numerical results, we exhibit that trust-based communication can greatly improve the performance of sensor-cloud. Finally, open research issues regarding trust-based communication for sensor-cloud are presented.

The rest of this article is organized as follows. We discuss the related work in terms of trust-based communication. We present the three types of trust-based communication mechanisms for sensor-cloud. An evaluation regarding trust-based communication for sensor-cloud is performed. The open research issues about trust-based communication for sensor-cloud are shown. This article is then concluded.

Related Work on Trust-Based Communication

Concerning smart meter, a concept named trusted smart meter is introduced in [6] for protecting the private information of consumers from the terminal end. Particularly, for hiding the platform configuration of smart meters, attribute certificates are utilized. For hiding the personal information of users, ring signature technology is utilized.

About smart grid, the trust system placement issue is investigated in [7] from the perspective of network topology. Specifically, a scheme is developed to defend the supervisory control and data acquisition networks with minimal number of trust nodes. A network segmentation approach is utilized to distribute the trust nodes, while linear programming problem formulations and local search are utilized to compute trust nodes.

For smart home, a system that employs logic, brain-computer interfacing, and sensor agents is designed in [8] utilizing epistemic logic and the logic of trust, the communication between the person and the sensor agents with a brain-computer interfacing headset is enabled.

Regarding smart campus, an architecture based on trusted execution environments for secure access control is shown in [9]. Incorporating identity-based encryption mechanisms, the challenges for establishing the architecture are

Chunsheng Zhu is with Nanjing Agricultural University and the University of British Columbia; Joel J. P. C. Rodrigues is with the National Institute of Telecommunications (Inatel), Instituto de Telecomunicações, ITMO University, and the University of Fortaleza (UNI-FOR); Victor C. M. Leung is with the University of British Columbia; Lei Shu (corresponding author) is with Nanjing Agricultural University and the University of Lincoln; Laurence T. Yang is with St. Francis Xavier University.

Digital Object Identifier: 10.1109/MCOM.2018.1700592

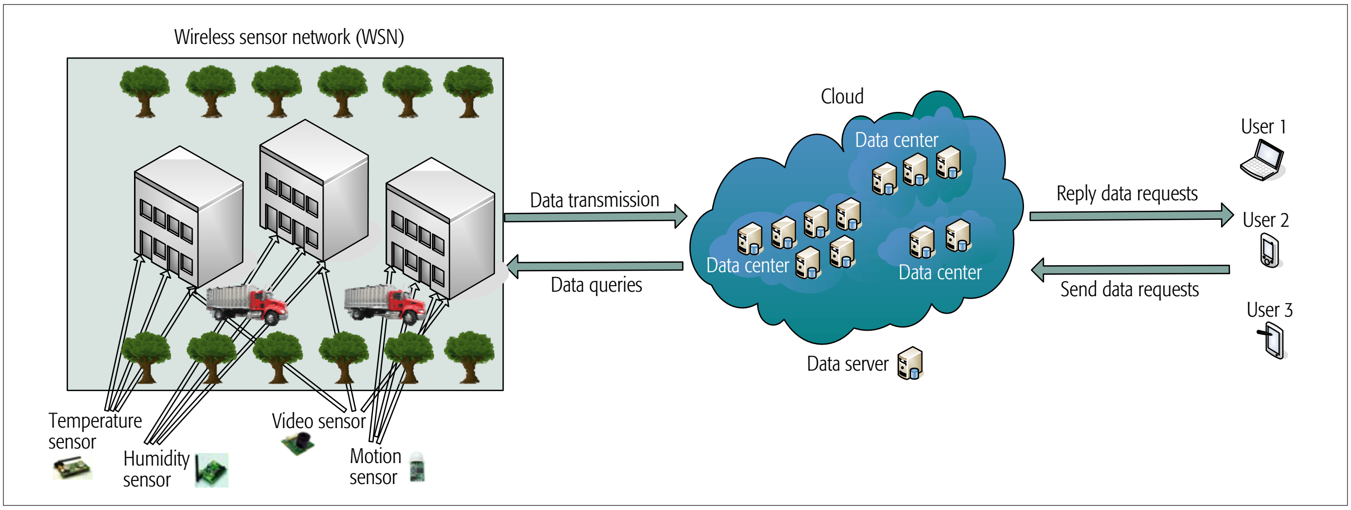

Figure 1. An instance of sensor-cloud.

identified. In addition, the potential benefits of the architecture are presented.

With respect to smart city, a trust service platform is leveraged for data usage control in [10]. Specifically, a trust-based usage control approach is established to enable the stakeholders to set the access control policies, considering their trust relationships with the data consumers. The roles and the interactions of the components of the trust-based usage control approach are also exhibited.

Three Types of Trust-Based Communication Mechanisms for Sensor-Cloud

In this section, sensor-cloud is presented first, followed by the introduction of the three kinds of trust-based communication mechanisms for sensor-cloud — independent sensor-cloud (ISC), collaborative sensor-cloud (CSC), and mutual sensor-cloud (MSC) — considering trust value and trust value threshold.

Sensor-Cloud

As a paradigm of IIoT, sensor-cloud [5] is for the intelligent operation and communication of the wireless sensor network (WSN) and the cloud by integrating them, to conveniently offer desirable sensory data to users so that people can be better served. Particularly, as shown in Fig. 1 on sensor-cloud, by connecting and interacting the WSN and the cloud, the data sensed and gathered by the ubiquitous sensor nodes in the WSN can be transmitted to the cloud first, followed by the powerful storage and processing of the data centers in the cloud. Eventually, the processed sensory data can be delivered on demand to users from the cloud anytime and anywhere if there is Internet connection. These delivered sensory data are for satisfying the information needs of people.

Independent Sensor-Cloud

As shown in Table 1, for ISC, the sensor nodes' trust values and data centers' trust values are determined by the WSN and the cloud independently. The trust value thresholds of sensor nodes and data centers are also chosen by the WSN and the cloud independently. The detailed process is shown as follows.

1. The WSN obtains the trust value of each sensor node, and the cloud achieves the trust value of each data center through trust value calculation methods [11].
2. In each time epoch:
   –Whether the transmission path can be formed in the WSN, the trust value thresholds of sensor nodes are determined by the WSN.
   –Whether the task can be fulfilled in the cloud, the trust value thresholds of data centers are chosen by the cloud. After the trust value thresholds of sensor nodes and data centers are selected, the trusted sensor nodes and trusted data centers are used in the WSN and the cloud, respectively.
3. From the WSN to the cloud, the sensory data is gathered and transmitted. From the cloud to the users, the sensory data is stored, processed, and further delivered on demand.

	Features
ISC	Sensor nodes' trust values and trust value thresholds are determined by WSN. Data center's trust values and trust value thresholds are determined by cloud.
CSC	Sensor nodes' trust values are determined by WSN. Sensor nodes' trust value thresholds are determined by the collaboration of WSN and cloud. Data centers' trust values are determined by cloud. Data centers' trust value thresholds are determined by the collaboration of WSN, cloud, and users.
MSC	Sensor nodes' trust values and trust value thresholds are determined by WSN. Data centers' trust values and trust value thresholds are determined by cloud. There are trust values, regarding WSNs and clouds as well as users. There are mutual trust value thresholds, among WSNs and clouds as well as users.

Table 1. Features of ISC, CSC, and MSC.

Collaborative Sensor-Cloud

Regarding CSC, as presented in Table 1, steps 1 and 3 of CSC are the same as those of ISC, but not step 2 of CSC. Namely, regarding the trust value threshold selection in step 2 of CSC, WSN not only considers whether the transmission path can be formed in WSN, but also incorporates the

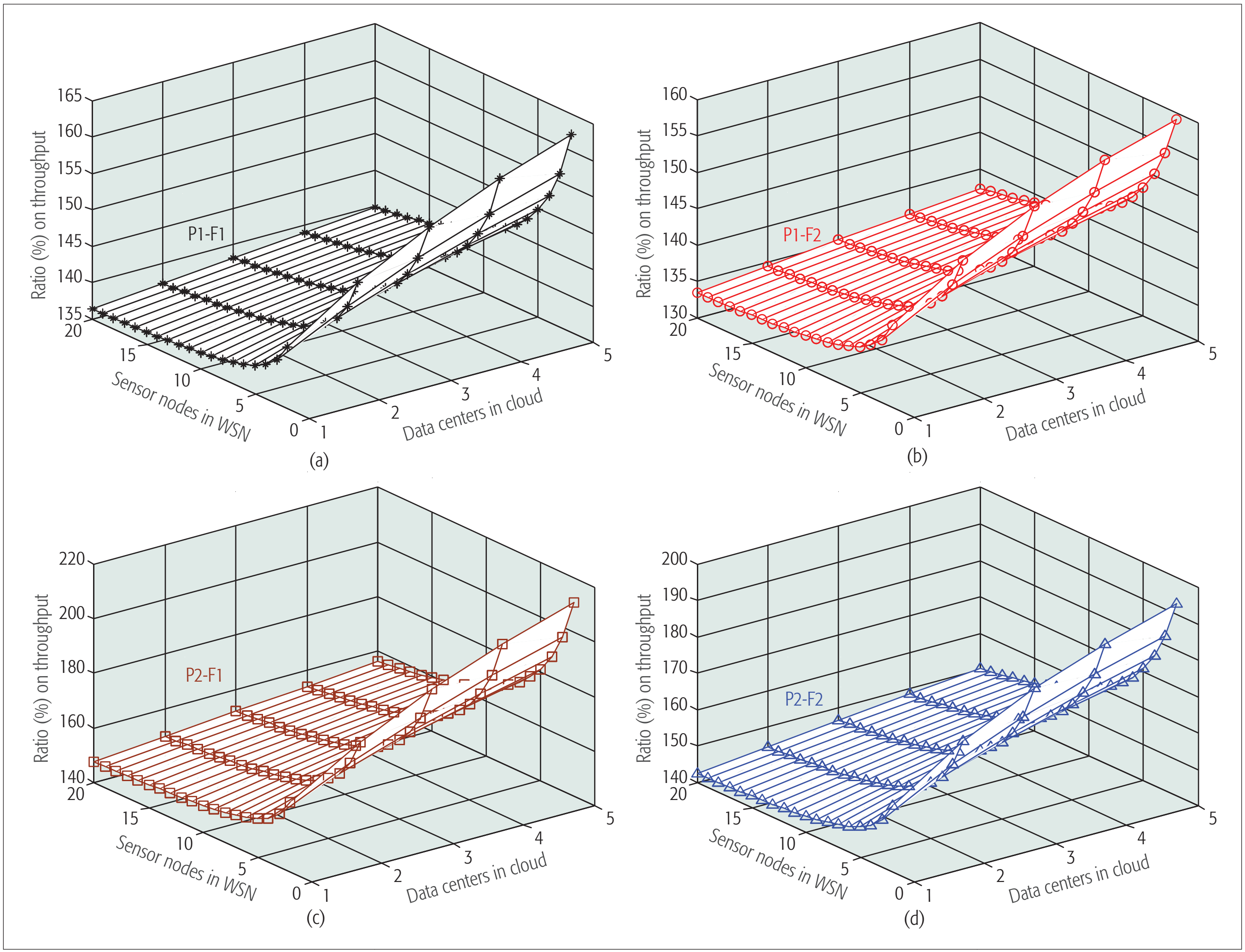

Figure 2. TSC to NTSC ratio (%) on throughput in Scenario 1: a) P1-F1; b) P1-F2; c) P2-F1; and d) P2-F2.

previous interactions with the cloud resulting from various sensor nodes' trust value thresholds in the history. Similarly, the cloud takes into account both whether the task can be fulfilled in the cloud and the previous interactions with the WSN and users, led by different data centers' trust value thresholds in the past.

In other words, comparing CSC with ISC, the trust values of sensor nodes and data centers are both chosen by the WSN and the cloud independently. However, the trust value thresholds of sensor nodes are determined by the collaboration of WSN and cloud in CSC. The trust value thresholds of data centers are determined by the collaboration of WSN, cloud and users in CSC. Collaborating WSN and cloud as well as users during the trust value threshold selection procedure, is to choose more appropriate trust value thresholds, considering the previous interactions among the WSN, the cloud and the users triggered by different trust value thresholds in the history.

MUTUAL SENSOR-CLOUD

In ISC and CSC, it is only assumed that

- There are trust values of the sensor nodes in the WSN and trust values of the data centers in the cloud
- There are trust value thresholds about the sensor nodes in the WSN and trust value thresholds about the data centers in the cloud.

In MSC, apart from the above, as demonstrated in Table 1, it is supposed that

- There are trust values regarding the WSN (V_{WSN}), the cloud (V_{Cloud}) and the user (V_{User});
- There are mutual trust value thresholds between WSNs and clouds as well as users.

Specifically, in MSC, sensor nodes' trust values and trust value thresholds are determined by the WSN. Data centers' trust values and trust value thresholds are determined by the cloud. The trust values of the WSN (V_{WSN}), the cloud (V_{Cloud}) and the user (V_{User}), can be achieved with the trust and reputation management system (e.g., [12]). The mutual trust value thresholds among WSNs and clouds as well as users, are determined by them mutually. For example, the trust value threshold d_3 for WSN to choose cloud is determined by WSN. The trust value threshold d_4 for cloud to select WSN is chosen by the cloud. Similarly, the trust value threshold d_5 for cloud to trust user is cloud's decision and the trust value threshold d_6 for user to trust cloud is user's decision.

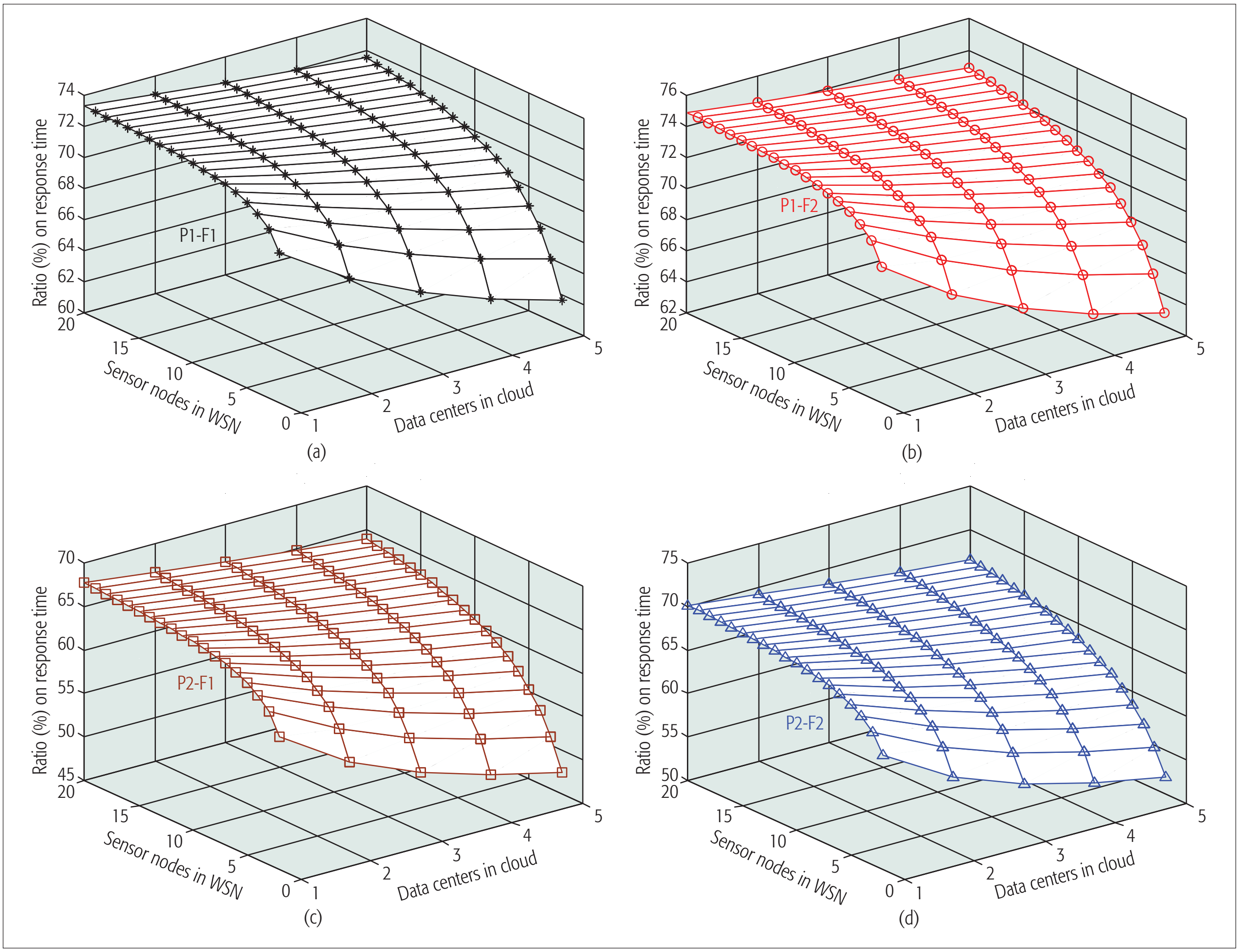

Figure 3. TSC to NTSC ratio (%) on response time in Scenario 1: a) P1-F1; b) P1-F2; c) P2-F1; and d) P2-F2.

The detailed steps of MSC are presented as below.

- Comparing V_{WSN}s, V_{Cloud}s, V_{User}s with d_3s, d_4s, d_5s, d_6s (e.g., V_{WSN} needs to surpass d_4; V_{Cloud} needs to surpass d_3 and d_6; V_{User} needs to surpass d_5), each WSN chooses the cloud(s) it trusts. Similarly, each cloud selects the WSN(s) and the user(s) it trusts. Each user chooses the trusted cloud(s). With this process, the mutual trust between WSNs and clouds as well as users, are established. Namely, the WSNs and clouds as well as users trust each other mutually.
- Step 1) of ISC
- Step 2) of ISC
- Step 3) of ISC

About V_{WSN}, V_{Cloud}, V_{User}, they actually mean the confidence that WSN, cloud and user have shown to each other facing uncertainty in future transactions. Regarding the mutual trust value thresholds, d_3 and d_6 together determine whether the cloud is qualified to deal with the sensory data from WSN as well as handle the data requests from user. d_4 and d_5, determine whether the WSN and the user are trustworthy, respectively. By utilizing V_{WSN}s, V_{Cloud}s, V_{User}s and d_3s, d_4s, d_5s, d_6s, WSNs and clouds as well as users will start mutual transactions with more confidence.

Evaluation About Trust-Based Communication for Sensor-Cloud

Determining the effectiveness of trust-based communication about enhancing the QoS that the sensory data is achieved by users from sensor-cloud, trust-based communication for sensor-cloud (TSC) is in contrast to non-trust-based communication for sensor-cloud (NTSC). Performed with a simulation tool named NetTopo, the throughput and response time are utilized as the evaluation metrics and the detailed evaluation is presented as below.

Evaluation Setup

The sensor-cloud system includes one WSN, one cloud, and 10 users. One sink node, one source node and 100 normal sensors nodes are included in the WSN, with a date rate which is 1000 kb/s. The WSN transmits the sensory data to the cloud including 10 data centers. Sensory data in the cloud is further requested on demand by each user. Each time epoch is 1 s.

In general, the sensor nodes' trust values and the data centers' trust values surpass certain thresholds, in TSC. The sensor nodes' trust values and the data centers' trust values are random values ranging from 0 and 1, in NTSC.

The following two scenarios show the detailed information regarding the evaluation.

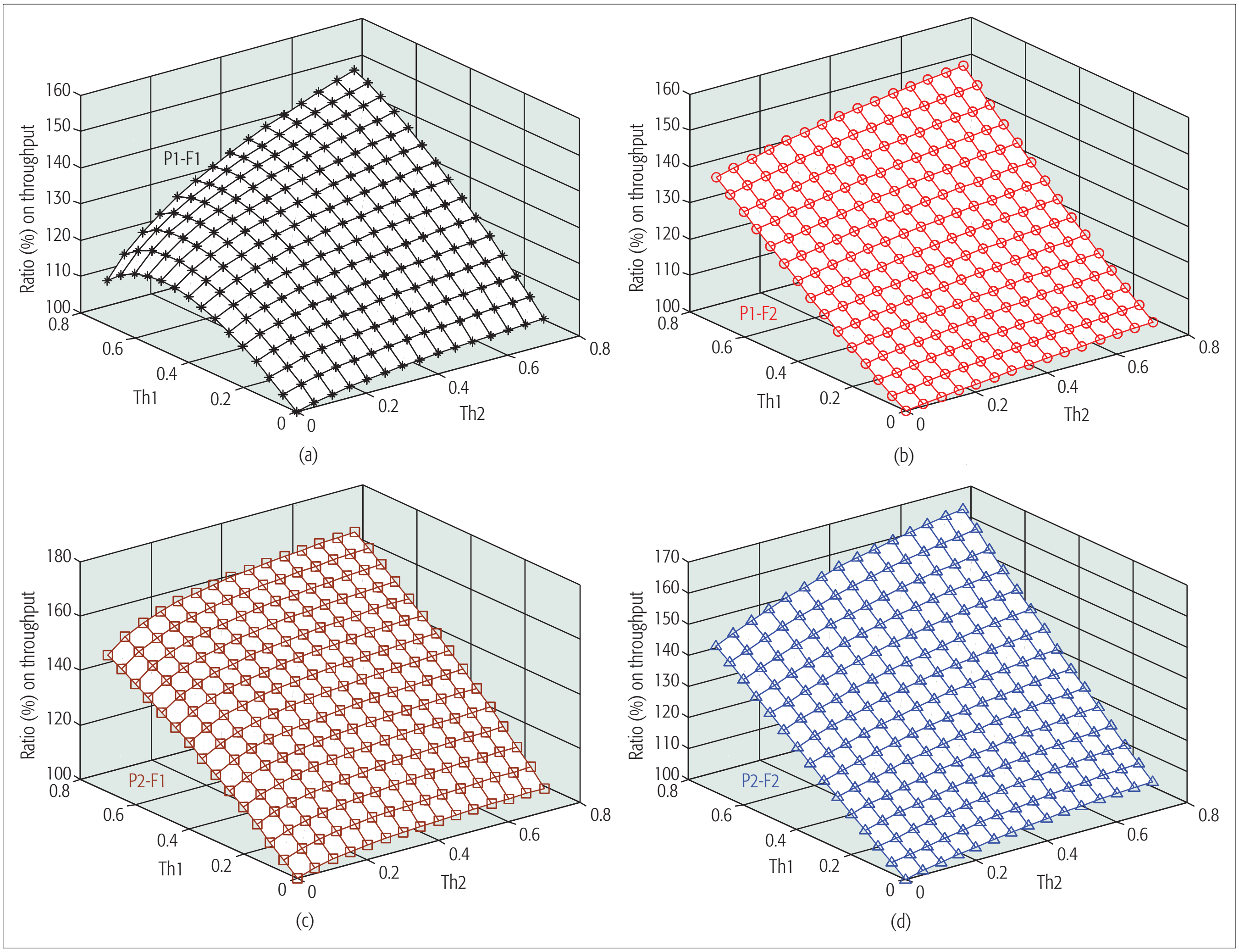

Figure 4. TSC to NTSC ratio (%) on throughput in Scenario 2: a) P1-F1; b) P1-F2; c) P2-F1; and d) P2-F2.

Scenario 1: For comparing the throughput and response time of TSC and NTSC, 100 simulations with various topologies are utilized. In these topologies, the number of sensor nodes changes from 1 to 20 and the number of data centers changes from 1 to 5 in the sensor-cloud transmission path, for both TSC and NTSC. About TSC, both sensor nodes' trust value thresholds and data centers' trust value thresholds are set to be 0.5. In terms of NTSC, each sensor node's trust value and each data center's trust value are always random values ranging from 0 and 1.

Scenario 2: For analyzing trust value thresholds' impacts on throughput and response time, a specific topology in which the sensor-cloud transmission path includes 10 sensor nodes and 2 data centers is utilized, for both TSC and NTSC. For this topology, the sensor nodes' trust value thresholds and data centers' trust value thresholds are varied 7 times (from 0.0 to 0.7) in TSC. Particularly, for each time, the trust value threshold is increased by 0.1 in TSC. Meanwhile, each sensor node's trust value and each data center's trust value are still always random values, ranging from 0 and 1 in NTSC.

In particular, the TSC to NTSC ratios (%) on the throughput and the response time resulting from the same topology (i.e., the same distribution-function combination) are utilized to compare the performance of TSC and NTSC, since it is more fair that the analysis is based on the throughput and response time regarding the same topology. Denoting uniform distribution and normalized exponential distribution by P1 and P2 respectively as well as representing inverse function and negative exponential function with F1 and F2 respectively, four distribution-function combinations (i.e., P1-F1, P1-F2, P2-F1, P2-F2) are achieved and analyzed.

Evaluation Results

Regarding the TSC to NTSC ratios (%) on throughput and response time in Scenario 1, Fig. 2a–2d and Fig. 3a–3d depict the evaluation results, respectively. Particularly, from these figures, it can be obviously achieved that in different topologies, the throughput of TSC nearly always outperforms the throughput of NTSC a lot. In the meantime, the response time of TSC almost always substantially falls behind the response time of NTSC.

Moreover, with respect to the TSC to NTSC ratios (%) on throughput and response time in Scenario 2, Fig. 4a–4d and Fig. 5a–5d describe the evaluation results, respectively. It can be obtained from those figures that in terms of different trust value thresholds, TSC still owns larg-

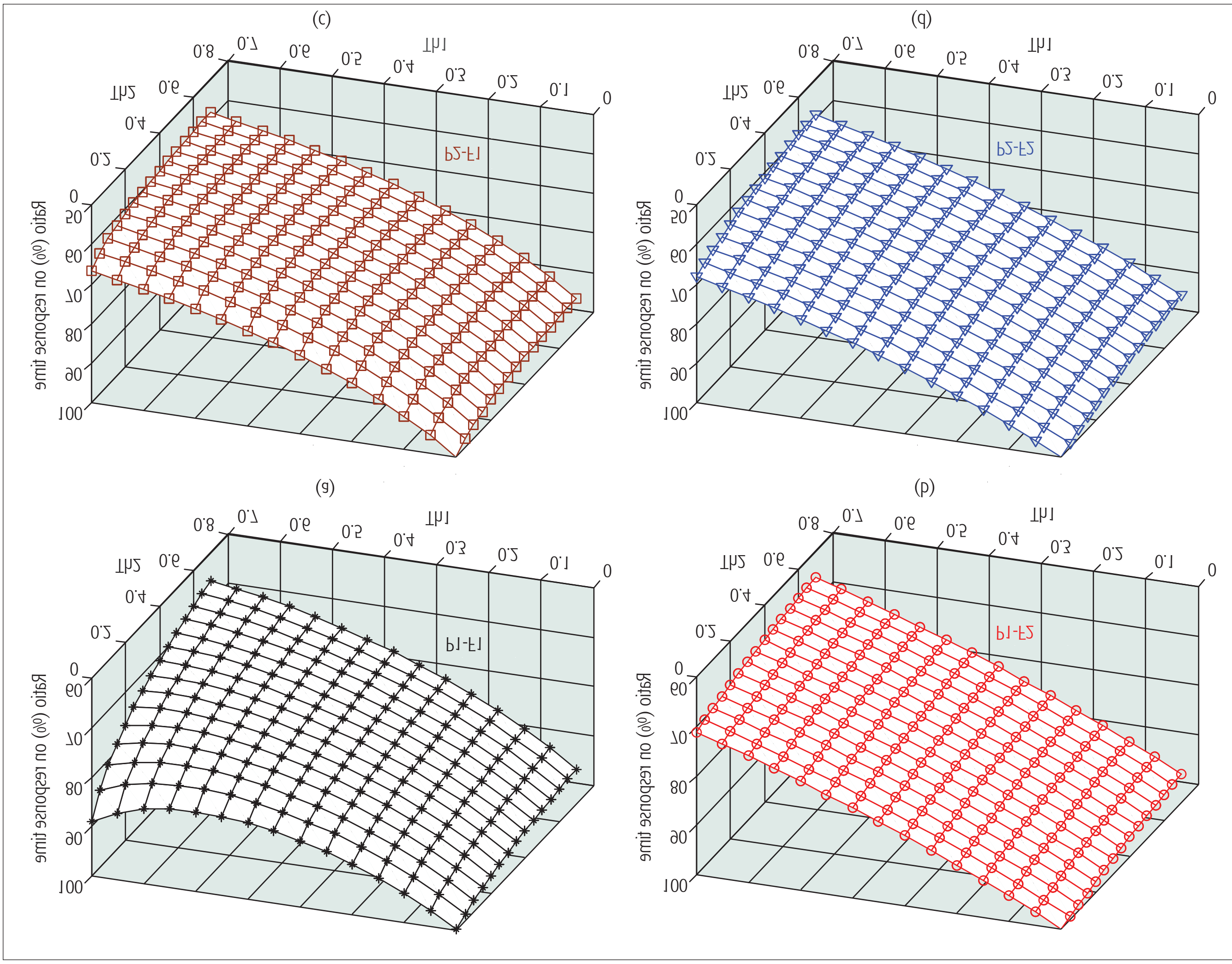

Figure 5. TSC to NTSC ratio (%) on response time in Scenario 2: a) P1-F1; b) P1-F2; c) P2-F1; and d) P2-F2.

er throughput than NTSC, while TSC still owns smaller response time than NTSC. In particular, the TSC to NTSC ratio (%) on throughput can be increased and the TSC to NTSC ratio (%) on response time can be decreased, by growing the trust value thresholds in general. Based on all the evaluation results, it is achieved that the performance of sensor-cloud can be greatly enhanced with trust-based communication.

Open Research Issues on Trust-Based Communication for Sensor-Cloud

Trust-Based Communication for Mobile Sensor-Cloud: For mobile sensor-cloud [13] in which sensor-cloud has mobility of sensors, the process that determines which entity can be trusted will be impacted by the mobile sensors. Particularly, how to compute the trust value of entities considering the mobility of sensors is worth studying.

Trust-Based Communication for Underwater Sensor-Cloud: Regarding underwater sensor-cloud [14], the collection of evidence regarding the trustworthiness of entities is performed underwater. In such a case, factors (e.g., acoustic propagation) might affect the gathering process. In addition, the evaluation of the trust values of entities should consider the underwater environment.

Trust-Based Communication for Green Sensor-Cloud: With respect to green sensor-cloud [15], in which sensor-cloud is for green monitoring or control, the trust-based communication should be in accordance with the greenness requirement while satisfying the QoS. Specifically, if the QoS has to do with particular attention to monitoring accuracy, accuracy oriented trust-based green communication probably will be adopted in real application scenarios.

Trust-Based Communication for Social Sensor-Cloud: In terms of social sensor-cloud where sensor-cloud is for a social group, it is necessary to consider the trustworthiness of the people in the social group, while taking into account the trustworthiness of the entities in the sensor-cloud. In particular, the trust evaluation of the social group members and the trust evaluation of the sensor-cloud entities might influence each other.

Conclusion

In this article, focusing on the performance of IIoT, we have explored trust-based communication for IIoT. Specifically, we have proposed three types of trust-based communication mechanisms (ISC, CSC, and MSC) for sensor-cloud, which is a paradigm of IIoT. Moreover, we have shown that trust-based communication can greatly enhance

In terms of social Sensor-Cloud where Sensor-Cloud is for a social group, it is necessary to consider the trustworthiness of the people in the social group, while taking into account the trustworthiness of the entities in the Sensor-Cloud.

the performance of sensor-cloud with numerical results. Finally, we have presented the open research issues regarding trust-based communication for sensor-cloud.

Acknowledgments

This work was partially supported by a Four Year Doctoral Fellowship from the University of British Columbia and funding from the Natural Sciences and Engineering Research Council of Canada, the ICICS/TELUS People & Planet Friendly Home Initiative at the University of British Columbia, TELUS, and other industry partners. The work of J. J. P. C. Rodrigues was supported by National Funding from the FCT – Fundação para a Ciência e a Tecnologia through the UID/EEA/500008/2013 Project, by the Government of the Russian Federation, Grant 074-U01, and by Finep, with resources from Funttel, Grant No. 01.14.0231.00, under the Centro de Referência em Radiocomunicações — CRR project of the Instituto Nacional de Telecomunicações (Inatel), Brazil. The work of L. Shu was supported by Maoming Engineering Research Center of Industrial Internet of Things (No. 517018) and International and Hong Kong, Macao, and Taiwan collaborative innovation platforms, and by major international cooperation projects of colleges in Guangdong Province (Grant No.2015KGJHZ026). The corresponding author is Lei Shu.

References

[1] L. D. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Trans. Ind. Info.*, vol. 10, no. 4, Nov. 2014, pp. 2233–43.

[2] M. Dong *et al.*, "LSCD: A Low-Storage Clone Detection Protocol for Cyber-Physical Systems," *IEEE Trans. Comp.-Aided Design Integrated. Circuits Sys.*, vol. 35, no. 5, May 2016, pp. 712–23.

[3] H. Yu *et al.*, "A Survey of Trust and Reputation Management Systems in Wireless Communications," *Proc. IEEE*, vol. 98, no. 10, Oct. 2010, pp. 1755–72.

[4] Y. Liu *et al.*, "Activetrust: Secure and Trustable Routing in Wireless Sensor Networks," *IEEE Trans. Info. Forensics Security*, vol. 11, no. 9, Sept. 2016, pp. 2013–27.

[5] C. Zhu *et al.*, "Multimethod Data Delivery for Green Sensor-Cloud," *IEEE Commun. Mag.*, vol. 55, no. 5, May 2017, pp. 176–82.

[6] J. Zhao *et al.*, "Privacy Protection Scheme Based on Remote Anonymous Attestation for Trusted Smart Meters," *IEEE Trans. Smart Grid*, Nov. 2016.

[7] M. M. Hasan and H. T. Mouftah, "Optimal Trust System Placement in Smart Grid Scada Networks," *IEEE Access*, vol. 4, May 2016, pp. 2907–19.

[8] V. Tulceanu, "A Matter of Trust: Smart Home System Relying on Logic, BCI, and Sensor Agents," *Proc. 17th Int'l. Symp. Symbolic Numeric Algorithms for Scientific Comp.*, 2015, pp. 177–80.

[9] M. A. Bouazzouni *et al.*, "Trusted Access Control System for Smart Campus," *Proc. Int'l. IEEE Conf. Ubiq. Intell. & Comp., Advanced Trusted Comp,, Scalable Comp. Commun., Cloud Big Data Comp., Internet of People, Smart World Congress*, 2016, pp. 1006–12.

[10] N. B. Truong *et al.*, "Leverage a Trust Service Platform for Data Usage Control in Smart City," *Proc. IEEE GLOBECOM* 2016, pp. 1–7.

[11] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 14, no. 2, 2nd qtr. 2012, pp. 279–98.

[12] C. Zhu *et al.*, "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," *IEEE Trans. Info. Forensics Security*, vol. 10, no. 1, Jan. 2015, pp. 118–31.

[13] R. Kumar and S. Rajalakshmi, "Mobile Sensor Cloud Computing: Controlling and Securing Data Processing over Smart Environment Through Mobile Sensor Cloud Computing (MSCC)," *Proc. Int'l. Conf. Comp. Sci. Appl.*, 2013, pp. 687–94.

[14] C. Srimathi, S.-H. Park, and N. Rajesh, "Proposed Framework for Underwater Sensor Cloud for Environmental Monitoring," *Proc. 5th Int'l. Conf. Ubiq. Future Net.*, 2013, pp. 104–09.

[15] T. Ojha *et al.*, "Dynamic Duty Scheduling for Green Sensor-Cloud Applications," *Proc. IEEE 6th Int'l. Conf. Cloud Comp. Tech. Sci.*, 2014, pp. 841–46.

Biographies

CHUNSHENG ZHU is a visiting scholar in the College of Engineering at Nanjing Agricultural University in China, and a postdoctoral research fellow in the Department of Electrical and Computer Engineering at the University of British Columbia, Canada. He received his Ph.D. degree in electrical and computer engineering from the University of British Columbia in 2016. His current research interests mainly include wireless sensor networks, cloud computing, the Internet of Things, social networks, and security.

JOEL J. P. C. RODRIGUES is a professor and senior researcher at the National Institute of Telecommunications (Inatel), Brazil, and a senior researcher at the Institute of Telecommunication, Portugal. He is the Editor-in-Chief of three international journals, and a co-author of over 500 papers, three books, and two patents. He is the recipient of several Outstanding Leadership and Outstanding Service Awards from IEEE Communications Society and several best paper awards.

VICTOR C. M. LEUNG [F] is a professor in the Department of Electrical and Computer Engineering and holder of the TELUS Mobility Research Chair at the University of British Columbia. His research is in the areas of wireless networks and mobile systems. Dr. Leung is a Fellow of the Royal Society of Canada, a Fellow of the Canadian Academy of Engineering, and a Fellow of the Engineering Institute of Canada.

LEI SHU is a Distinguished Professor in the College of Engineering at Nanjing Agricultural University in China, and a Lincoln Professor in the School of Engineering at the University of Lincoln, United Kingdom. He is an Associate Editor of *IEEE Transactions on Industrial Informatics*, *IEEE Systems Journal*, and *IEEE Access*. His research interests include wireless sensor networks and cloud computing.

LAURENCE T. YANG is a professor in the Department of Computer Science, St. Francis Xavier University, Canada. His research interests include parallel and distributed computing, embedded and ubiquitous/pervasive computing, and big data. He has published more than 220 papers in various refereed journals (around 40 percent in top IEEE/ACM transactions and journals). His research has been supported by the National Sciences and Engineering Research Council and the Canada Foundation for Innovation.