

Improved Reliability of Communication in Cellular Internet of Things through Consensus

Shin-Hung Pan¹ and Shu-Ching Wang^{2*}

¹Department of M-Commerce and Multimedia Applications, Asia University,
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan, R.O.C.

²Department of Information Management, Chaoyang University of Technology,
168, Jifeng E. Rd., Wufeng, Taichung 413310, Taiwan, R.O.C.

(Received November 23, 2020; accepted January 8 2021)

Keywords: cellular Internet of Things, edge computing, consensus problem

With the establishment and large-scale use of fifth-generation (5G) wireless networks, it is foreseeable that the Cellular Internet of Things (CIoT) will be applied in various fields. For instance, there are a large number of sensors for temperature measurement and cameras for video capture in cities. To provide highly reliable CIoT services, a reliable communication network must be designed. One of the commonly used methods to design a reliable communication network in a distributed system is to reach a consensus. However, none of the protocols proposed for the consensus problem in the past can be directly used in the network topology of CIoT. We propose an optimal protocol, the reliable communication medium consensus (RCMC), to reach a consensus on CIoT. The maximum number of abnormal communication media (CMs) in the CIoT topology is tolerated by the proposed RCMC, and only two data exchanges need to be performed.

1. Introduction

Owing to the popularity of the Internet of Things (IoT) and the popularization of 4G/5G, the data-processing mode of many IoT-related application services is gradually changing. To achieve ubiquitous access to IoT, cellular networks and wireless sensor networks (WSNs) have been integrated. Edge computing (EC) is a computing paradigm in which data are processed at the edge of the network. Through EC, large amounts of computing power and storage space distributed at the edge of the network are collected to generate sufficient resources to provide related services on mobile devices.⁽¹⁾ Therefore, EC and IoT can be implemented in dense cellular networks to establish a practical Cellular Internet of Things (CIoT) platform. Since CIoT with EC is one of the most promising technologies in 5G cellular systems,⁽²⁾ through CIoT with EC, everything can be connected to the Internet. Vukobratovic *et al.* proposed a feasible CIoT topology in 2019.⁽³⁾ Their proposed CIoT topology can realize an integrated platform of EC and IoT in a dense cellular network, so the service performance of the CIoT platform can be improved. In this study, the CIoT platform proposed by Vukobratovic *et al.* was applied and

*Corresponding author: e-mail: scwang@gm.cyut.edu.tw
<https://doi.org/10.18494/SAM.2021.3196>

redefined as ECIoT (CIoT based on EC). Because EC distributes computing and storage resources from centralized clouds to distributed edge servers to support various applications that require low latency, ECIoT can provide more diverse IoT-related applications and services.

To increase the reliability of ECIoT to achieve different application service requirements of distributed computing, secure and highly reliable communication is one of the topics that must be discussed to provide high-quality ECIoT services. Reaching a consensus is one of the commonly used design methods to improve the reliability of distributed systems. So far, there has been no relevant research on ECIoT involving the consensus problem of abnormal network communication. This paper gives the first ever discussion of the consensus protocol for the topology of ECIoT with abnormal communication media (CMs).

The solution to the consensus problem is to define a protocol so that all normal processing units (PUs) can reach a consensus and use the minimum number of data exchanges with the maximum number of allowable abnormal components. In this paper, the solution to the consensus problem is re-discussed in the context of ECIoT. The definition of the problem is to make all PUs in ECIoT reach a consensus. Our newly designed protocol allows each PU of CIoT to select an initial data as a starting point when executing the protocol and to communicate with all other PUs by exchanging data. If the following conditions are met, the PUs have reached a consensus:⁽⁴⁾

Consensus: All PUs agree on a common data.

Validity: If the initial data of each PU_i is v_i , then all PUs agree on the data v_i .

Many related studies on the consensus problem are based on the assumption that the PU is abnormal in a reliable network.⁽⁵⁾ From this assumption, regardless of whether the PU is normal or not, the abnormality of the CMs will be regarded as the abnormality of the PU, so that the normal PU cannot reach a consensus. However, the definition of the consensus problem requires that all normal PUs must reach a consensus. Therefore, to provide CIoT with a reliable communication environment, ECIoT is used in this research. In ECIoT, many PUs are connected to each other. Even if some CMs are abnormal, all PUs must reach a consensus of the same data in ECIoT. We reconsider the consensus problem under the assumption that the CMs are abnormal in ECIoT. The proposed protocol to reach a consensus on ECIoT is called the reliable communication medium consensus (RCMC). The RCMC can solve the consensus problem in ECIoT by using the minimum number of data exchanges and increase the fault tolerance capability by allowing the maximum number of abnormal CMs.

This study is divided into six parts. In Sect. 1, the motivation and goals of this research are given. The topology of ECIoT is defined in Sect. 2. A detailed description of the proposed RCMC is given in Sect. 3. For ease of understanding, an example of executing the RCMC is given in Sect. 4. The optimality of the RCMC is proved in Sect. 5. Section 6 concludes this study.

2. Topology of ECIoT

Because IoT provides related applications and services through the connection of a large number of IoT sensors (IoT PUs), it is necessary to provide quality of service (QoS) for IoT applications through 5G wireless networks with high-speed transmission capabilities.⁽⁶⁾

Nowadays, CIoT is widely regarded as the basic application of 5G wireless networks and enables millions of IoT PUs to connect to a single base station (BS).⁽⁷⁾ The main function of an IoT PU is to sense and report relevant information in the environment. However, in some time-sensitive related applications, connecting an IoT PU directly to the Internet will not meet the time requirement. Therefore, some calculations and data will be hosted on a cellular BS in the form of an EC device (edge PU).⁽¹⁾

CIoT with EC can connect all IoT PUs to the Internet. The structure of ECIoT used in this study is shown in Fig. 1. ECIoT includes three tiers: an access tier, an edge tier, and a cloud tier.

A group of IoT PUs will form an access tier. For specific CIoT applications, IoT PUs are used to sense and report the required sensing signal. These IoT PUs within the coverage range of the BS will be connected to this specific BS. Then, all BSs are connected to the edge tier so that the edge PU in the edge cloud can obtain the required data to provide a specific application service.

The edge tier is organized into a group of edge clouds. Each edge cloud is responsible for processing the data required by a specific application and is composed of a large number of edge PUs. A cloud tier is formed by many cloud PUs, and related services required by cloud users will be provided by these cloud PUs. In ECIoT, various request data in real life will be collected through a large number of IoT PUs. With this huge amount of data, various CIoT-related applications and sequence services can be provided.

ECIoT is composed of many PUs that can communicate with each other. Even if some CMs fail due to internal damage or external intruders, it is necessary to reach a consensus on the same data in ECIoT so that the applications of ECIoT can still be executed normally. In this study, the PUs of ECIoT are reliable during the execution of the consensus, whereas the CMs may be abnormal due to noise or interference from hijackers, resulting in the exchange of data that may exhibit arbitrary behavior. When all PUs reach a consensus in ECIoT, the reliability of ECIoT can be enhanced.

Since ECIoT is built based on EC, the edge tier is responsible for the execution of data analysis and processing. In ECIoT, computing and storage resources are managed by the edge tier, so ECIoT can provide more computing and data storage resources for connected PUs. Owing to its characteristics, ECIoT is a platform that can provide various CIoT services and applications.

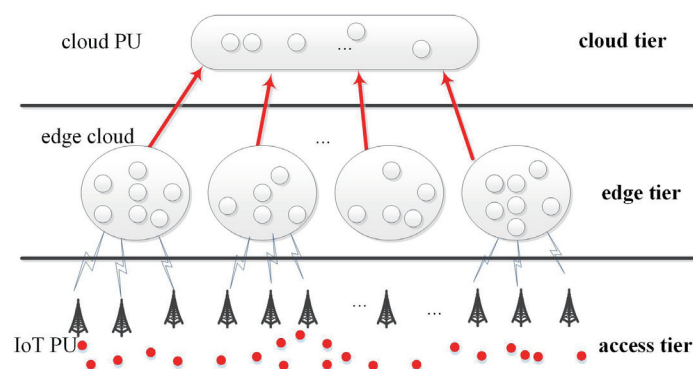


Fig. 1. (Color online) Structure of ECIoT.

3. Proposed Protocol

The purpose of a consensus protocol is to enable each normal PU in the network to reach a consensus. To reach a consensus, each PU should exchange data with all other PUs. Then, each PU collects enough data to determine the consensus data, and the consensus data of each PU must be the same.

In this study, the consensus problem of ECIoT is discussed. In the relevant research results on the consensus problem,^(4,5,8–10) the CM delay is not considered. Therefore, when the PU executes the protocol of solving the consensus, it should receive data from other PUs within a predictable time.⁽¹¹⁾ Therefore, if the PU does not receive the data in time, it means that the data have been affected by abnormal CMs.

The proposed RCMC is used to solve the consensus problem in ECIoT with abnormal CMs. On the basis of the three tiers of ECIoT, the proposed protocol RCMC is executed by the PUs in the order of access tier, edge tier, and cloud tier in the three-tier hierarchy. To provide CIoT-related services, the required data of a specific CIoT application are sensed by IoT PUs in ECIoT. Then, the sensed data are sent by the IoT PUs to the corresponding edge cloud in the edge tier. In the proposed method, the edge PU located in the edge cloud first receives the sensed data sent from the IoT PUs, and then the majority value of the received sensed data is calculated. The majority value of the received data is used as the initial data (v_i) of the edge PU_{*i*}, which is used to execute the RCMC. When each edge cloud obtains the consensus data separately, the data are expressed as the content of the specific service responsible for the edge cloud. Finally, the consensus data are transmitted to the cloud tier by the edge PUs. In ECIoT, the role of the cloud PUs in the cloud tier is to collect the results of different specific services, and then a consensus vector is obtained, thereby providing an integrated service center for various CIoT-related applications.

The proposed method is initiated by the IoT PUs of the access tier to obtain the sensed data of the specific application service. There are two stages of the proposed RCMC, the data-gathering stage and the consensus data determination stage. The parameters of the RCMC include v_i and n , where v_i is the initial data of PU_{*i*} and n is the number of PUs participating in the consensus. For all PUs to reach a consensus, each PU must collect enough exchanged data from all other PUs in the data-gathering stage to enable the consensus data to be determined in the consensus data determination stage. In the RCMC, the data-gathering stage only needs to perform two data exchanges to collect enough data. In the first data exchange, each PU_{*i*} multicasts its initial data v_i through CMs and then receives the initial data of other PUs. The initial data sent from other PUs received by each PU are stored in a vector, and each element in the vector corresponds to the PU that sent the data. In the second data exchange, each PU_{*i*} sends the vector V_i received in the first data exchange and constructs a matrix $[V_1, V_2, \dots, V_n]$, denoted by MAT_i , $1 \leq i \leq n$. Then, in the consensus data determination stage, the function MAJ_k is used to determine the consensus data DEC_i by taking the majority data of the k th row of MAT_i for $1 \leq k \leq n$. Finally, the consensus data DEC_i are used to reach a consensus for all PUs participating in the consensus. The detailed definition of the RCMC is shown in Fig. 2.

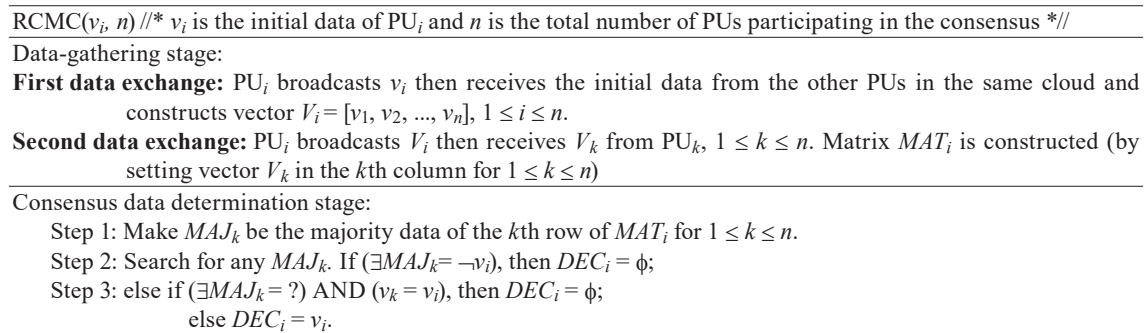


Fig. 2 Proposed protocol of RCMC.

4. Example of Executing RCMCM

We take the Agricultural Internet of Things (AIoT) constructed by ECIoT as an example to execute the RCMC as an example in this section. When ECIoT is applied to AIoT, by combining a large number of IoT PUs with different functions, sensor data required for various agricultural application services can be collected, and then the related services can be provided. In this example, there are five IoT PUs in the coverage of a specific BS_1 at the access tier, six edge PUs in edge cloud E_1 of the edge tier, and five cloud PUs in the cloud tier. Figure 3 shows the AIoT constructed by ECIoT used as an example.

First, each IoT PU in the access tier perceives the monitoring status. We assume that in the coverage of a specific BS_1 at the access tier, the CM between IoT PU u_{11} and the edge tier and the CM between u_{13} and the edge tier are abnormal. The sensing data of each IoT PU in B_1 at the access tier are shown in Fig. 4. The sensing monitoring statuses of B_1 at the access tier are transferred to edge cloud E_1 of the edge tier. Because the CM between u_{11} and the edge tier and the CM between u_{13} and the edge tier are abnormal, the data transmitted by the edge PU through the abnormal CMs will be arbitrarily changed. The data that has been arbitrarily modified are represented by bold and italics.

Each edge PU in edge cloud E_1 receives the sensing data transmitted from the IoT PUs within B_1 . When the edge PU receives the sensing data sent by the five IoT PUs, the majority value of these five sensing data is obtained by the edge PU. Next, the majority data (1) are used as the initial data (v_i) of the PU in edge cloud E_1 , and the proposed protocol $RCMC(v_i, n) = RCMC(1, 6)$ is executed. The initial data of each edge PU in edge cloud E_1 of the edge tier are shown in Fig. 4.

After that, the RCMC is executed by each edge PU in edge cloud E_1 . In the first data exchange of the data-gathering stage in the RCMC, each edge PU e_{ij} broadcasts v_i , and then receives the initial data from the other edge PUs in the same edge cloud, and constructs vector V_i . In this example, the CM between e_{11} and e_{15} and the CM between e_{12} and e_{14} are assumed to be abnormal. The vector received in the first data exchange of edge cloud E_1 of the edge tier is shown in Fig. 5. In the second data exchange of the data-gathering stage in the RCMC, edge PU e_{ij} broadcasts V_i , then receives the vectors broadcast by the other edge PUs and constructs MAT_i . After that, in the consensus data determination stage of the RCMC, the majority data of MAT_1

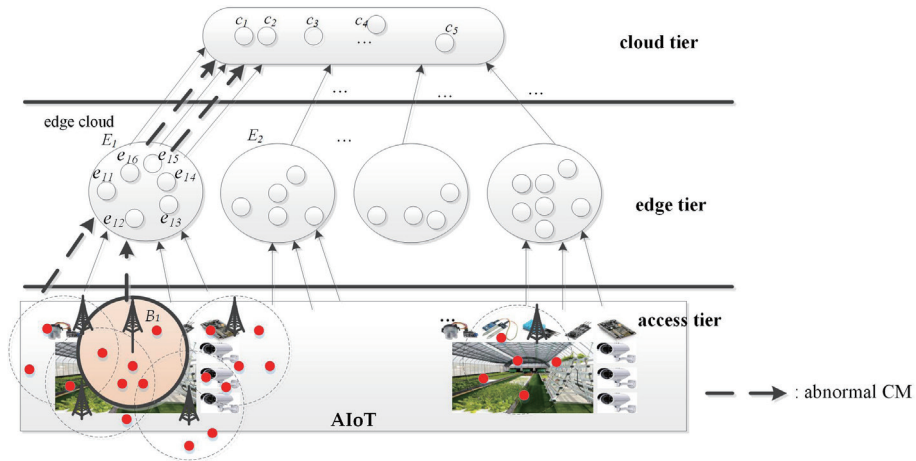


Fig. 3. (Color online) Example of AIoT constructed by ECIoT.

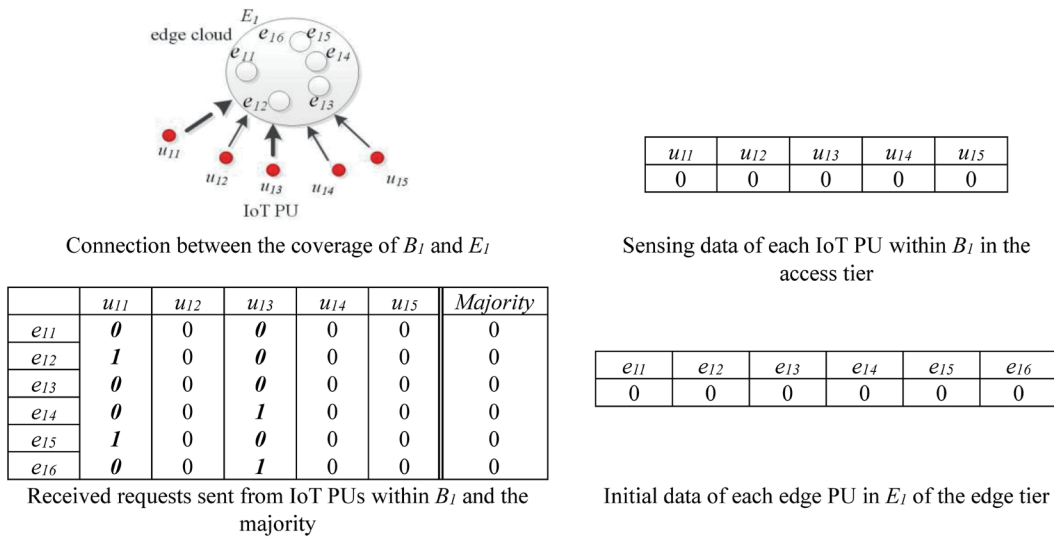


Fig. 4. (Color online) Initial data of each edge PU in edge cloud E_1 of the edge tier.

	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}
e_{11}	0	0	0	0	1	0
e_{12}	0	0	0	1	0	0
e_{13}	0	0	0	0	0	0
e_{14}	0	1	0	0	0	0
e_{15}	1	0	0	0	0	0
e_{16}	0	0	0	0	0	0

Fig. 5. Vector received in first data exchange of edge cloud E_1 of edge tier.

are used to construct the matrix MAJ_1 , and the common data $DEC_1 (= 0)$ are obtained for the edge PUs of edge cloud E_1 . MAT_1 is constructed in the second data exchange of the data-gathering stage in the RCMC, as shown in Fig. 6.

e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}	$DEC_{11}=0$	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}	$DEC_{12}=0$
0	0	0	0	1	0		0	0	0	0	1	0	
0	0	0	1	0	0		0	0	0	1	0	0	
0	0	0	0	0	0		0	0	0	0	0	0	
0	0	0	0	0	0		0	0	0	0	0	0	
0	1	0	0	0	0		1	1	1	0	1	0	
0	1	1	1	0	1		1	0	0	0	0	0	
MAJ_{11} of MAT_{11}							MAJ_{12} of MAT_{12}						
e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}	$DEC_{13}=0$	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}	$DEC_{14}=0$
0	0	0	0	1	0		0	0	0	0	1	0	
0	0	0	1	0	0		0	1	1	1	1	0	
0	0	0	0	0	0		0	0	0	0	0	0	
0	0	0	0	0	0		0	0	0	0	0	0	
0	1	0	0	0	0		0	1	0	0	0	0	
1	0	0	0	0	0		1	0	0	0	0	0	
MAJ_{13} of MAT_{13}							MAJ_{14} of MAT_{14}						
e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}	$DEC_{15}=0$	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}	$DEC_{16}=0$
1	1	1	1	1	1		0	0	0	0	1	0	
0	0	0	1	0	0		0	0	0	1	0	0	
0	0	0	0	0	0		0	0	0	0	0	0	
0	0	0	0	0	0		0	0	0	0	0	0	
0	1	0	0	0	0		0	1	0	0	0	0	
1	0	0	0	0	0		1	0	0	0	0	0	
MAJ_{15} of MAT_{15}							MAJ_{16} of MAT_{16}						

Fig. 6. Construction of MAT_1 in second data exchange, and MAJ_1 of MAT_1 used as common data.

	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}	Majority
c_1	0	0	0	1	0	0	0
c_2	0	1	0	0	0	0	0
c_3	0	0	0	0	0	0	0
c_4	0	1	0	0	0	0	0
c_5	0	1	0	1	0	0	0

Fig. 7. Consensus data of each cloud PU in cloud tier.

Finally, the consensus data of each edge PU in edge cloud E_1 are transferred to the cloud tier. In this example, the CM between e_{12} and the cloud tier and the CM between e_{14} and the cloud tier are assumed to be abnormal. The cloud PUs in the cloud tier receive the consensus data of each edge PU in edge cloud E_1 , and the majority value of the consensus data is taken by the cloud PU. The consensus data of each cloud PU in the cloud tier are shown in Fig. 7.

5. Optimality of the RCMC Protocol

The variables used when proving the optimality of the proposed method are listed in detail in Table 1. In previous studies,^(4,5,8-10) the number of allowable abnormal CMs in the consensus

Table 1
Variables used in this study.

Variable	Meaning
n_{BS}	Number of BSs in access tier
B_j	Coverage of specific BS_j at access tier, $1 \leq j \leq n_{BS}$
BS_j	Base station j at access tier
n_{Bj}	Number of IoT PUs in B_j at access tier
u_{ij}	IoT PU in B_j at access tier, $1 \leq i \leq n_{Bj}$
n_E	Number of edge clouds at edge tier
E_j	Edge cloud of edge tier, $1 \leq j \leq n_E$
n_{Ej}	Number of edge PUs in E_j of edge tier
e_{ij}	Edge PU in E_j of edge tier, $1 \leq i \leq n_{Ej}$
n_C	Number of cloud PUs in cloud tier
c_i	Cloud PU in cloud tier, $1 \leq i \leq n_C$
CM_{AEj}	Total number of CMs between B_j at access tier and E_j of edge tier
CM_{Ej}	Number of CMs in E_j of edge tier
CM_{ECj}	Number of CMs between E_j of edge tier and cloud PUs in cloud tier
F_{AEj}	Total number of allowable abnormal CMs between B_j at access tier and E_j of edge tier
F_{Ej}	Total number of allowable abnormal CMs in E_j of edge tier
F_{ECj}	Total number of allowable abnormal CMs between E_j of edge tier and cloud PUs in cloud tier

problem was determined by the total number of CMs in a distributed system. In the study of Wang *et al.*,⁽¹⁰⁾ it was proved that $\lceil (t - 1)/2 \rceil - 1$ abnormal CMs is the maximum number of allowed abnormalities, where t is the total number of CMs in the distributed system. Therefore, the constraints of the RCMC are given as follows.

- **(Constraint between access tier and edge tier):** $CM_{AEj} > \lfloor (CM_{AEj} - 1)/2 \rfloor + F_{AEj}$ is the constraint between the access tier and edge tier. This constraint specifies the number of CMs required between the access tier and edge tier.
- **(Constraint of edge tier):** $CM_{Ej} > \lfloor (CM_{Ej} - 1)/2 \rfloor + F_{Ej}$ is the constraint of the edge tier. This constraint specifies the number of CMs required in the edge cloud E_j of the edge tier.
- **(Constraint between edge tier and cloud tier):** $CM_{ECj} > \lfloor (CM_{ECj} - 1)/2 \rfloor + F_{ECj}$ is the constraint between the edge tier and cloud tier. This constraint specifies the number of CMs required between the edge tier and cloud tier.

By using the constraints of the RCMC, its optimality will be proved by the following theorems. The optimality of the RCMC is verified by considering the number of data exchanges and the number of tolerable abnormal CMs. Through the proofs of Theorems 1 and 2, the RCMC is proved to be the optimal solution to the consensus problem in ECIoT.

Theorem 1: If there is only one data exchange, there is not enough collected data to solve the consensus problem in ECIoT.

Proof: To reach a consensus among the PUs in ECIoT, data exchange is necessary. Since the PU cannot obtain abnormal data in other PUs without data exchange, the consensus problem cannot be solved. In addition, the data obtained in one data exchange are insufficient to solve the consensus problem. For example, if PU_i is connected to PU_j through an abnormal CM, PU_i only uses one data exchange without knowing the initial data in PU_j . Therefore, it is impossible to reach a consensus using only one data exchange.

Theorem 2: The total number of abnormal CMs allowed by the RCMC is optimal.

Proof: Since ECIoT is a three-tier topology, the total number of abnormal CMs allowed by the RCMC can be discussed through the three levels of ECIoT.

(1) CMs between access tier and edge tier: Since the number of abnormal CMs between B_j at the access tier and E_j of the edge tier cannot exceed half of the total number of CMs between the access tier and edge tier, the majority of the sensed data can be determined. Hence, letting F_{AE} be the total number of allowable abnormal CMs between B_j at the access tier and E_j of the edge tier, we have $F_{AE} = \sum_{j=1}^A F_{AEj}$ and $F_{AEj} \leq \lfloor (CM_{AEj} - 1)/2 \rfloor$.

(2) CMs in edge tier: Since in each edge cloud E_j of the edge tier, the total number of abnormal CMs cannot exceed half of the total number of CMs in the edge tier, the majority of data obtained by each edge cloud can be determined. Hence, letting F_E be the total number of allowable abnormal CMs in the edge tier, we have $F_E = \sum_{j=1}^E F_{Ej}$ and $F_{Ej} \leq \lfloor (CM_{Ej} - 1)/2 \rfloor$.

(3) CMs between edge tier and cloud tier: Since the number of abnormal CMs between E_j of the edge tier and the cloud tier cannot exceed half of the total number of CMs between the edge tier and cloud tier, the majority of the consensus data can be determined. Hence, letting F_{EC} be the total number of allowable abnormal CMs between the edge tier and cloud tier, we have $F_{EC} = \sum_{j=1}^E F_{ECj}$ and $F_{ECj} \leq \lfloor (CM_{ECj} - 1)/2 \rfloor$.

In short, the maximum number of abnormal CMs allowed by the RCMC is $F = F_{AE} + F_E + F_{EC} = \sum_{j=1}^A F_{AEj} + \sum_{j=1}^E F_{Ej} + \sum_{j=1}^E F_{ECj}$.

6. Conclusions

Because the solution of consensus problems is one of the most commonly used methods in the field of providing reliable distributed systems, many protocols have been proposed to solve the consensus problem for different network topologies.^(4,5,8-10) In this study, ECIoT with abnormal CMs was considered. The proposed protocol RCMC only requires two data exchanges, and the consensus of all PUs in ECIoT can be reached. Also, the RCMC can tolerate the maximum number of abnormal CMs in ECIoT.

In addition, as WSNs become part of IoT, a cluster of sensor nodes in a WSN can cooperate to achieve certain goals. In a cluster-based WSN (CWSN), each cluster is composed of many sensor nodes and a cluster head. The sink can control the status and communication data of all cluster heads. A tier composed of a cluster of sensor nodes and the cluster head can correspond to the access tier of ECIoT. The cluster head in the cluster of the access tier will be connected to the edge tier and can communicate with the sink. A tier composed of a set of sinks can correspond to the edge tier of ECIoT. Therefore, the RCMC proposed in this study can be directly applied to CWSNs.

Furthermore, only considering the consensus problem of abnormal CMs in ECIoT is still not enough to realize highly reliable ECIoT. This is because in actual ECIoT-related applications, there are not only abnormal CMs in the network topology but also abnormal PUs. Therefore, in

future research, the proposed protocol will be extended to solve the consensus problem for the case that abnormal CMs and PUs exist simultaneously in ECIoT.

Acknowledgments

This work was supported in part by the Ministry of Science and Technology (MOST 107-2221-E-324-005-MY3).

References

- 1 S. Dama, V. Sathya, K. Kuchi, and T.V. Pasca: IEEE Consum. Electron. Mag. **6** (2016) 66. <https://ieeexplore.ieee.org/document/7786962>
- 2 G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz: IEEE Access **6** (2017) 3619. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8141874>
- 3 D. Vukobratovic, D. Bajovic, K. Anoh, and B. Adebisi: Proc. 2019 IEEE Int. Conf. Communications (IEEE, 2019) 1–7.
- 4 F. J. Meyer and D. K. Pradhan: IEEE Trans. Parallel Distrib. Syst. **2** (1991) 214. <https://doi.org/10.1109/71.89066>
- 5 M. Fischer, M. Paterson, and N. Lynch: J. ACM **32** (1985) 374. <https://doi.org/10.1145/3149.214121>
- 6 R. Jia, X. Chen, C. Zhong, D.W.K. Ng, H. Lin, and Z. Zhang: IEEE J. Sel. Top. Signal Process. **13** (2019) 538. <https://ieeexplore.ieee.org/abstract/document/8637821>
- 7 O. Liberg, M. Sundberg, E. Wang, J. Bergman, and J. Sachs: Cellular Internet of things: Technologies, standards, and performance, Academic Press (Elsevier, USA, 2017).
- 8 M. Fischer, M. Paterson, and N. Lynch: J. ACM. **32** (1985) 374. <https://dl.acm.org/doi/abs/10.1145/3149.214121>
- 9 L. Lamport, R. Shostak, and M. Pease: ACM Trans. Program. Lang. Syst. **4** (1982) 382. <https://dl.acm.org/doi/abs/10.1145/3335772.3335936>
- 10 S. C. Wang, S. C. Tseng, and K. Q. Yan: ICIC Express Lett. Part B, Appl. Int. J. Res. Surv. **8** (2017) 937. <https://ci.nii.ac.jp/naid/40021187503/>
- 11 X. Li, X. Chen, and Y. Xie: Math. Probl. Eng. (2015). <https://doi.org/10.1155/2015/957028>

About the Authors



Shin-Hung Pan received his M.S. and Ph.D. degrees from the Department of Information Management, Chaoyang University of Technology, Taiwan. Currently, he is an assistant professor with the Department of M-Commerce and Multimedia Applications, Asia University, Taiwan. His current research interests include cloud computing, edge computing, and IoT. (vincentpan@asia.edu.tw)



Shu-Ching Wang received her M.S. degree in electrical engineering from National Chen-Kung University and her Ph.D. degree in information engineering from National Chiao-Tung University, Taiwan. Currently, she is a professor with the Department of Information Management, Chaoyang University of Technology, Taiwan. Her current research interests include distributed computing, cloud computing, and IoT. (scwang@gm.cyut.edu.tw)