ICIC Express Letters
Part B: Applications
Volume **9**, Number **12**, December **2018**

ICIC International ©2018 ISSN 2185-2766
pp. **1209–1216**

THE OPTIMAL SOLUTION OF CONSENSUS IN A FOG COMPUTING BASED IOT WITHIN UNRELIABLE COMMUNICATION

Shu-Ching Wang, Ya-Jung Lin and Kuo-Qin Yan*

Department of Information Management
Chaoyang University of Technology
168, Jifeng E. Rd., Wufeng District, Taichung 41349, Taiwan
{ scwang; s10614903 }@cyut.edu.tw; *Corresponding author: kqyan@cyut.edu.tw

Received August 2018; accepted October 2018

Abstract. *The Internet of Things (IoT) is a network of physical things, objects, or devices. Because Fog computing is an emergency architecture for computing, storage, control, and networking, these services can be distributed to the cloud to the end users of the IoT. It covers both mobile and wired scenarios; hence, it can support the application of IoT. However, to be able to provide IoT applications, a high reliable IoT platform must be supported. However, the previous protocols for the consensus problem of distributed computing are not enough for the IoT platform combining Fog computing and Cloud computing. In this study, the consensus problem is revisited. The new proposed protocol, FC Consensus (FCC) protocol, can make all fault-free nodes reach consensus with minimal rounds of message exchanges and tolerate the maximal number of allowable faulty components in the IoT platform combining Fog computing and Cloud computing.*
Keywords: Internet of Things, Fog computing, Cloud computing, Consensus

1. **Introduction.** The IoT is based on intelligent and self-configuring nodes (things) interconnected in a dynamic and global network infrastructure. IoT facilitates new interactions among things and humans, and enables the realization of smart cities, infrastructures, and services that enhance the quality of life. IoT is generally characterized by real world and small things with limited storage and processing capacity, and consequential issues regarding reliability, performance, security, and privacy [1]. Since, Cloud computing has virtually unlimited capabilities in terms of storage and processing power, hence it has most of the IoT issues at least partially solved. Therefore, the IT paradigm that combines the two technologies of cloud and IoT can provide current and future Internet.

Cloud computing is an Internet-based computing paradigm that provides ubiquitous and on-demand access to a shared pool of configurable resources to other computers or devices. Although the cloud-computing paradigm is able to handle huge amounts of data from IoT clusters, the transfer of enormous amounts of data to and from cloud computers presents a challenge because of limited bandwidth. Consequently, the need arises to process data near the data source, and Fog computing provides a promising solution to this problem [2].

Fog computing is a novel trend in computing that aims to process data near the data source. It pushes applications, services, data, computing power, and decision making away from the centralized nodes to the logical extremes of a network. Fog computing significantly decreases the data volume that must be moved between end devices and the cloud, and it enables data analytics and knowledge generation to occur at the data source. Furthermore, the dense geographic distribution of fog helps to attain better localized accuracy for many applications as compared to the cloud [3].

DOI: 10.24507/icicelb.09.12.1209

In order to provide a high flexible and reliable platform of IoT, an IoT platform combining Fog computing and Cloud computing (FC-IoT) is used in this study. Achieving consensus on a same value in the FC-IoT even if certain transmission media (TMs) are fallible, the protocol is required so that systems can still operate correctly. In previous studies, the consensus algorithms were designed in traditional network topology [4-7]. Those works reach consensus underlying different topologies respectively, including fully connected network [4], multicasting network [5], wireless sensor network [6], and cloud computing environment [7]. All those previous protocols are not suitable for FC-IoT due to the difference of network topology. To enhance fault-tolerance of FC-IoT, in this study, the consensus is revisited with the assumption of malicious faulty TMs in FC-IoT. The proposed protocol, FC Consensus (FCC) protocol of FC-IoT, can make all fault-free nodes reach consensus with minimal rounds of message exchanges, and tolerate the maximal number of allowable faulty TMs.

The rest of this paper is organized as follows. Section 2 will serve to introduce the basic concepts of the consensus problem and the FC-IoT used in this study. The proposed FCC of FC-IoT will be brought up and illustrated in detail in Section 3. An example of executing FCC is also given in this section. Section 4 is responsible for proving the complexity of our new protocol. Finally, Section 5 gives conclusions of this research.

2. Related Works.

Before the consensus problem can be solved, two basic concepts must be made and clearly defined in advance. They are the consensus problem and the structure of FC-IoT.

2.1. The consensus problem.

In an IoT environment, a mechanism to allow a given set of nodes to agree on a common value is necessary for reliable smart city [8]. Such a unanimity problem was called *consensus* [9]. In our study, the *consensus* problem of FC-IoT will be explored.

The *consensus* problem is defined by Meyer and Pradhan [9]. The solutions of *consensus* problem are defined as protocols, which achieve a consensus and hope to use the minimum number of rounds of message exchanges to achieve the maximum number of allowable faulty capability. The definition of the problem is to make the fault-free nodes in the FC-IoT reach consensus. Each node chooses an initial value to start with, and communicates to each other by exchanging messages. The nodes are referred to make a consensus if it satisfies the following conditions [9].

Consensus: All fault-free nodes agree on a common value.

Validity: If the initial value of each fault-free node n_i is v_i then all fault-free nodes shall agree on the value v_i.

In a consensus problem, many cases are based on the assumption of node failure [10]. Based on this assumption, a TM fault is treated as a node fault, whatever the fault-freeness of an innocent node, so an innocent node does not involve consensus [11]. The symptom of a faulty TM can be classified into two types: dormant and malicious. A dormant faulty TM always can be identified by the receiver if the transmitted message was encoded appropriately before transmission. The message transmitted by the malicious faulty TM is random or arbitrary. This is the most destructive type of failure and leads to the most serious problems. That is, if the consensus problem can be resolved in the case of a malicious fault, then the consensus problem can also be resolved in other failure modes. Therefore, the consensus problem is revisited with the assumption of TM failure on malicious faults in the FC-IoT in this study.

2.2. The network structure.

In order to provide a high flexible and reliable platform of IoT, an IoT platform combining Fog computing and Cloud computing (FC-IoT) is used in this study. The topology of FC-IoT is shown in Figure 1. There are three layers in the FC-IoT: *IoT sensors layer*, *Fog computing layer* and *Cloud computing layer*. The IoT sensors

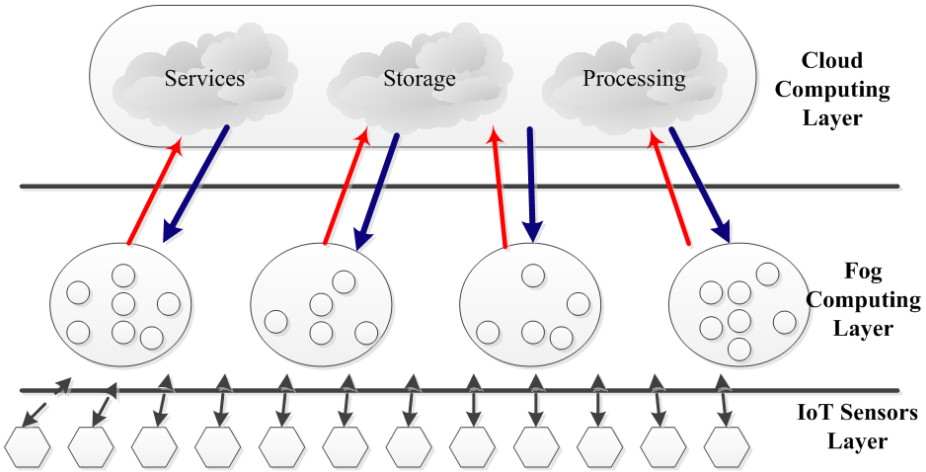


FIGURE 1. The topology of FC-IoT

layer is composed of sensor nodes, which is responsible for sensing the data required by the IoT application. The Fog computing layer is constructed by Fog groups; each Fog group is composed of a large number of Fog nodes, responsible for the processing of specific information. The Cloud computing layer is made up of many Cloud nodes, which provide Cloud users' services.

The FC-IoT is proposed by Fog computing, where data can be analyzed and processed by devices in the network rather than being centralized in the Cloud computing. By coordinating and managing the computing and storage resources at the edge of the network, more and more connected devices and the emerging needs of IoT can be processed by the Fog computing. The Fog computing can be made as an appropriate platform for providing the critical services and applications of IoT [3].

3. **The Proposed Protocol.** In this study, the consensus problem is discussed in the FC-IoT; no delay of nodes or TMs is included in our discussion. Therefore, the nodes executing our new protocol should receive the messages from other nodes within a predictable period of time. If the message is not received on time, the message must have been influenced by faulty components.

There are two parts of FCC; one is main procedure and the other is procedure *Consensus*(v_i). The main procedure is used to get the requests for the application services and trigger procedure *Consensus*(v_i) to execute. The procedure *Consensus*(v_i) is used to get the Consensus value. And, there are two phases of procedure *Consensus*(v_i): the *message exchange phase* and *decision making phase*. The message exchange phase is used to collect messages from Fog nodes. Furthermore, the influence of a faulty TM can be removed. Afterward, in the decision making phase, each fault-free Fog node uses the messages received during the message exchange phase to determine the common Consensus value.

FCC only needs two rounds of message exchanges to solve the consensus problem. In the message exchange phase, each node communicates with other nodes. Finally, the decision making phase will reach consensus among the nodes. In the first round of the message exchange phase, each Fog node f_{ij} multicasts its initial value v_i, and then receives the initial value of other nodes. In the second round, each node f_{ij} sends the vector received in the first round, and constructs a matrix (MAT_i, $1 \leq i \leq n_{Fj}$). Finally, the decision making phase will reach consensus among the nodes. The proposed FCC is shown in Figure 2. In the FCC, MAT_i is the matrix set up at node f_{ij} for $1 \leq i \leq n_{Fj}$. The MAJ_k and DEC_i are used in procedure *Consensus* to determine the Consensus value. MAJ_k is a majority function that takes the majority value of the k-th row of MAT_i for $1 \leq k \leq n_{Fj}$.

FCC

/*Main*/

1) The requests for the application services are sent to the corresponding Fog group of Fog computing layer by IoT sensor nodes.
2) The Fog node f_{ij} receives the requests sent from sensor nodes, and the received requests are taken as the majority.
3) The majority value is used as the initial value (v_i) of f_{ij}.
4) The Fog nodes of Fog computing layer execute procedure $Consensus(v_i)$.
5) The Consensus value obtained from procedure $Consensus(v_i)$ is transferred to Cloud computing layer.
6) The Cloud nodes of Cloud computing layer get the Consensus values received from the Fog nodes of Fog computing layer and take the majority value.

Procedure Consensus(v_i)

Message Exchange Phase:

Round 1: Node f_{ij} broadcasts v_i, and then receives the initial value from the other nodes in the same group, and construct vector V_i.

Round 2: Node f_{ij} broadcasts V_i, and then receives the vectors broadcast by other nodes, and MAT_i is constructed by the following steps.

Step 1: Receive the initial value v_i from node f_{ij}, for $1 \leq i \leq n_{Fj}$.

Step 2: Construct the vector $V_i = [v_1, v_2, \ldots, v_n]$, $1 \leq i \leq n_{Fj}$.

Step 3: Broadcast V_i to all nodes, and receive column vector V_k from node f_{kj}, $1 \leq k \leq n_{Fj}$.

Step 4: Construct a MAT_i (Setting the vector v_k in column k for $1 \leq k \leq n_{Fj}$).

Decision Making Phase:

Step 1: Take the majority value of the k-th row of MAT_i to MAJ_k for $1 \leq k \leq n_{Fj}$.

Step 2: Search for any MAJ_k. If ($\exists MAJ_k = \neg v_i$), then $DEC_i := \phi$.

Step 3: Else if ($\exists MAJ_k$ =?) AND ($v_{ki} = v_i$), then $DEC_i := \phi$; else $DEC_i := v_i$ and terminate.

FIGURE 2. The proposed FCC

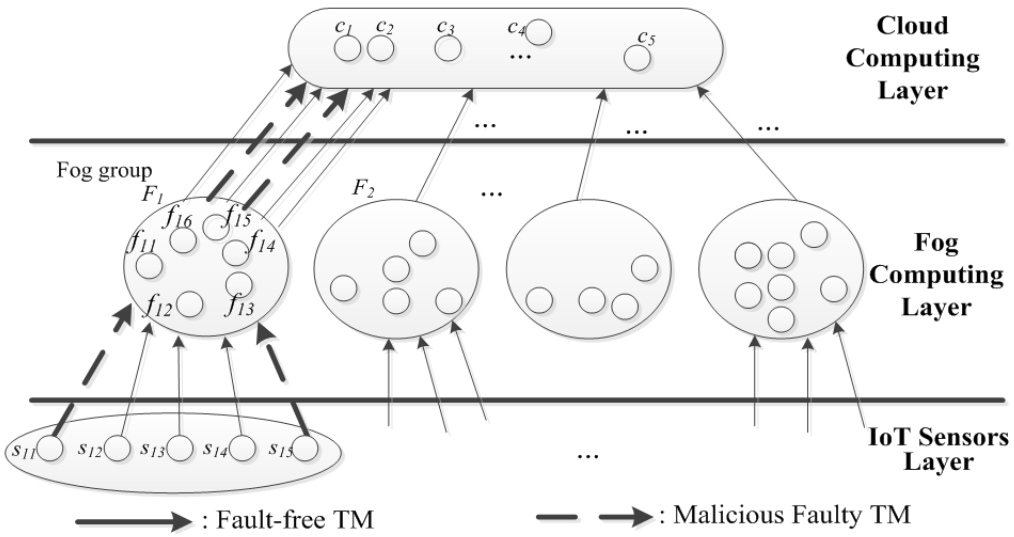
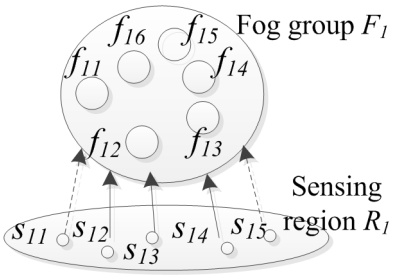


FIGURE 3. An example of FC-IoT

Finally, the Consensus value of each Fog node in Fog group F_1 is transferred to Cloud computing layer. In this example, the TM between f_{12} and Cloud computing layer, the TM between f_{14} and Cloud computing layer are assumed in malicious fault. The Cloud nodes in Cloud computing layer receive the Consensus value of each Fog node in Fog group F_1, and the received Consensus values are taken as the majority. The majority value is consensus value of Fog group F_1 and is shown in Figure 8.

4. **The Complexity of the FCC Protocol.** The following theorems are used to prove the complexity of FCC. The complexity of FCC is evaluated in terms of 1) the minimal number of rounds of message exchanges, and 2) the maximum number of allowable faulty components.



s_{11}	s_{12}	s_{13}	s_{14}	s_{15}
1	1	1	1	1

FIGURE 4. The sensing data of each sensor node in the IoT sensors layer

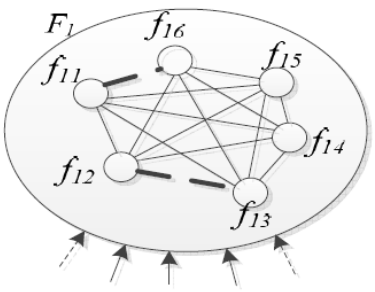
	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}	*Majority*
f_{11}	***1***	1	1	1	***0***	1
f_{12}	***0***	1	1	1	***0***	1
f_{13}	***1***	1	1	1	***1***	1
f_{14}	***0***	1	1	1	***1***	1
f_{15}	***1***	1	1	1	***0***	1
f_{16}	***0***	1	1	1	***0***	1

The received requests sent from sensor nodes and the majority

f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1	1	1	1	1	1

The initial value of each Fog node

FIGURE 5. The initial value of each Fog node in Fog group F_1



	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
f_{11}	1	1	1	1	1	***0***
f_{12}	1	1	***0***	1	1	1
f_{13}	1	***0***	1	1	1	1
f_{14}	1	1	1	1	1	1
f_{15}	1	1	1	1	1	1
f_{16}	***0***	1	1	1	1	1

FIGURE 6. The vector received in first round of Fog group F_1

f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1	1	1	1	1	0
1	1	0	1	1	1
1	0	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
1	***0***	***0***	***0***	***0***	***0***
1	1	1	1	1	1

MAJ_{11} of MAT_{11}

DEC_{11} =1

f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1	1	1	1	1	0
1	1	0	1	1	1
0	***0***	***0***	***0***	***0***	***0***
1	1	1	1	1	1
1	1	1	1	1	1
0	1	1	1	1	1
1	1	1	1	1	1

MAJ_{12} of MAT_{12}

DEC_{12} =1

f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1	1	1	1	1	0
0	***0***	***0***	***0***	***0***	***01***
1	0	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
0	1	1	1	1	1
1	1	1	1	1	1

MAJ_{13} of MAT_{13}

DEC_{13} =1

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

MAJ_{14} of MAT_{14}

DEC_{14} =1

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

MAJ_{15} of MAT_{15}

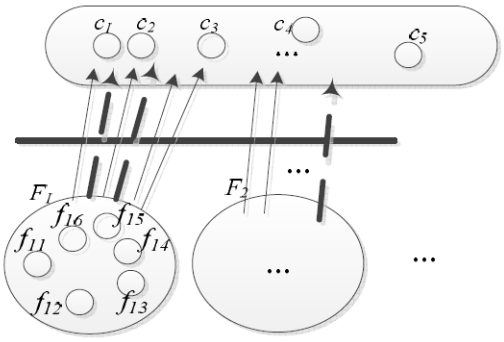
DEC_{15} =1

f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	***0***	***1***	***0***	***0***	***0***
1	1	0	1	1	1
1	0	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
0	1	1	1	1	1
1	1	1	1	1	1

MAJ_{16} of MAT_{16}

DEC_{16} =1

FIGURE 7. Construct MAT_1 in second round and MAJ_1 of MAT_1 as decision value



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

FIGURE 8. The consensus value of each node in Cloud computing layer

Theorem 4.1. *One round of message exchange cannot solve the consensus problem.*

Proof: Message exchange is necessary. A node cannot derive whether or not a disagreeable value exists in other nodes without message exchanging. Therefore, the consensus problem cannot be implemented. In addition, one round of message exchange is not enough to solve the consensus problem. If node n_i is connected with node n_m by faulty TM, node n_i may not know the initial value in node n_m by using only one round of message exchanges. Hence, it is possible to reach a consensus by using one round of message exchanges.

Theorem 4.2. *The total number of allowable faulty TMs by FCC is optimal.*

Proof: The total number of allowable faulty TMs by FCC can be discussed by three parts.

1) **TMs between IoT sensors layer and Fog computing layer**: The number of faulty TMs between sensing region R_j and Fog group F_j does not exceed half, and the majority value of the sensing data can be determined. Therefore, F_{RF} is the total number of allowable faulty TMs between IoT sensors layer and Fog computing layer. $F_{RF} = \sum_{j=1}^{R} f_{RFj}$ where R is the total number of sensing regions and f_{RFj} is the total number of allowable malicious faulty TMs between sensing region R_j and Fog group F_j. In addition, $f_{RFj} \leq \lfloor (TM_{RFj} - 1)/2 \rfloor$ where TM_{RFj} is the number of TMs between sensing region R_j and Fog group F_j.
2) **TMs in Fog computing layer**: The number of faulty TMs in each Fog group F_j does not exceed half, and the majority value of the Fog groups can be determined. Therefore, F_F is the total number of allowable faulty TMs in Fog computing layer. $F_F = \sum_{j=1}^{F} f_{Fj}$ where F is the total number of Fog groups and f_{Fj} is the total number of allowable malicious faulty TMs in Fog group F_j. In addition, $f_{Fj} \leq \lfloor (TM_{Fj} - 1)/2 \rfloor$ where TM_{Fj} is the number of TMs in Fog group F_j.
3) **TMs between Fog computing layer and Cloud computing layer**: The number of faulty TMs between Fog group F_j and Cloud computing layer does not exceed half, and the majority value of the consensus value can be determined. Therefore, F_{FC} is the total number of allowable faulty TMs between Fog computing layer and Cloud computing layer. $F_{FC} = \sum_{j=1}^{F} f_{FCj}$ where F is the total number of Fog groups and f_{FCj} is the total number of allowable malicious faulty TMs between Fog group F_j and Cloud computing layer. In addition, $f_{FCj} \leq \lfloor (TM_{FCj} - 1)/2 \rfloor$ where TM_{FCj} is the number of TMs between Fog group F_j and Cloud computing layer.

In short, the maximum number of allowable faulty components by FCC is $F_{total} = F_{RF} + F_F + F_{FC}$.

5. Conclusion.

In this study, the consensus problem was redefined by the FCC protocol in an FC-IoT paradigm. The proposed protocol ensures that all nodes in the network can reach a common value to cope with the influences of the faulty TMs by using the minimum number of message exchanges, while tolerating the maximum number of faulty TMs at any time.

Furthermore, only considering TM faults in the consensus problem is insufficient for the highly reliable FC-IoT. In the real world, not only might TMs be faulty, node might be faulty. Therefore, our protocol will be extended to reach consensus in a generalized case when faulty TMs or nodes exist simultaneously in the underlying FC-IoT in future work.

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

REFERENCES

[1] A. Botta, W. De Donato, V. Persico and A. Pescapé, On the integration of cloud computing and Internet of things, *Proc. of the 2014 International Conference on Future Internet of Things and Cloud*, pp.23-30, 2014.

[2] A. Munir, P. Kansakar and S. U. Khan, IFCIoT: Integrated fog cloud IoT: A novel architectural paradigm for the future Internet of things, *IEEE Consumer Electronics Magazine*, vol.6, no.3, pp.74-82, 2017.

[3] F. Jalali, S. Khodadustan, C. Gray, K. Hinton and F. Suits, Greening IoT with fog: A survey, *Proc. of IEEE International Conference on Edge Computing*, pp.25-31, 2017.

[4] K. Q. Yan, S. C. Wang and Y. H. Chin, Consensus under unreliable transmission, *Information Processing Letters*, vol.69, pp.243-248, 1999.
[5] K. Alekeish and P. Ezhilchelvan, Consensus in sparse, mobile ad hoc networks, *IEEE Trans. Parallel and Distributed Systems*, vol.23, no.3, pp.467-474, 2012.
[6] M. K. Maggs, S. G. O'keefe and D. V. Thiel, Consensus clock synchronization for wireless sensor networks, *IEEE Sensors Journal*, vol.12, no.6, pp.2269-2277, 2012.
[7] S. S. Wang and S. C. Wang, The consensus problem with dual failure nodes in a cloud computing environment, *Information Sciences*, vol.279, pp.213-228, 2014.
[8] J. Jin, J. Gubbi, S. Marusic and M. Palaniswami, An information framework for creating a smart city through Internet of things, *IEEE Internet of Things Journal*, vol.1, no.2, pp.112-121, 2014.
[9] F. J. Meyer and D. K. Pradhan, Consensus with dual failure modes, *IEEE Trans. Parallel and Distributed Systems*, vol.2, no.2, pp.214-222, 1991.
[10] L. Lamport, R. Shostak and M. Pease, The Byzantine general problem, *ACM Trans. Programming Languages and Systems*, vol.4, no.3, pp.382-401, 1982.
[11] S.-C. Wang, S.-C. Tseng and K.-Q. Yan, To achieve optimal trustworthy agreement in the unreliable mobile cloud computing environment, *ICIC Express Letters, Part B: Applications*, vol.8, no.6, pp.937-943, 2017.