A Malicious Agreement in a Cluster-based Wireless Sensor Network

S.C. Wang, K.Q. Yan*, C.L. Ho, S.S. Wang*

Department of Information Management, Chaoyang University of Technology
168, Jifeng E. Rd., Wufeng District, Taichung, 41349 Taiwan, R.O.C.
{scwang; kqyan; s10033902; sswang}@cyut.edu.tw
*: Corresponding author

Abstract—A Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions. Usually, as they are deployed to an open and unprotected region, they are vulnerable to various types of attacks. For wireless networks, a stable topology is an important research topic that provides good environment for transmission data in WSN. Further, the fault-tolerance and reliability of the WSN has been an important topic. The problem of reaching agreement in the distributed system is one of the most important issues to design a fault-tolerance system. In previous works, reach a common agreement among healthy nodes to cope with the influence from faulty components is significant in a fault-tolerance system. In this study, the agreement problem is revisited in a WSN, which the sensor nodes maybe subject to Byzantine (malicious) failure.

Keywords—Byzantine failure, Distributed system, Fault tolerant, Wireless sensor network

1. INTRODUCTION

Recently, the Micro-Electro-Mechanical Systems (MEMS) continues to grow at a high rate of speed in Wireless Sensor Networks (WSNs) [3]. However, the sensor node is limited by the energy resource, the memory, the computation, and the communication capability, etc. [6,17]. WSN is a distributed system that comprises thousands sensor nodes and sink. The characteristics of a WSN include small-scale sensor nodes, limited power, mobility, dynamic network topology, wireless communication, etc. [2,5,8,15,16,19-21,26]. However, the sensor nodes will collect the information and deliver it back to the sink node by using multi-hop wireless links from a specific region or nature environment. Moreover, WSN is a non-infrastructure network, there are two states of each sensor: move and fixed [2,3,11,14]. If there are sensor node leave from the original network, then it will communicate with each neighbor sensor node and try to become a new brief network topology. In other word, the network topology will be reconfigured in any necessitous times.

Nowadays, the WSN is practical more and more due to it can provide sensor node joins to the network or leaves away anytime with non-infrastructure. A group of sensor nodes in WSN is cooperating to achieve some objectives; each sensor node communicates with other sensor nodes by using broadcast in WSN, but also leads to a severe problem, such as broadcast storm [4]. Many researchers proposed cluster schemes and broadcast limited to prevent the broadcast storm [22]. However, the clustering topology has been proposed to prolong the lifetime of WSNs by decreasing the energy consumption of sensor nodes [1].

In this paper, the Byzantine Agreement problem is revisited with the assumption of sensor node failure on malicious faults in the Cluster-based Wireless Sensor Network (CWSN). The proposed protocol, Malicious Agreement Protocol (MAP), can make all healthy sensor nodes reaching agreement with minimal rounds of message exchange and tolerate the maximal number of allowable components.

The remainder of this paper is organized as follows. Section 2 discusses the WSN and the related work for Byzantine Agreement problem. Section 3 illustrates the concept of MAP by an example. Section 4 proves the correctness and demonstrates the complexity of the new protocol. Finally, Section 5 concludes this study.
2. RELATED WORK

Recent advances in technology have provided portable nodes with wireless interfaces that allow networked communication among mobile users. The computing environment, which refers to as mobile computing, no longer requires users to maintain a fixed and universally known position in the network and enables almost unrestricted mobility. The network topology of our research and the related results of agreement problem have discussed in this section.

2.1. The Topology of Cluster-based Wireless Sensor

As WSNs need not any infrastructure to provide the multi-hop wireless links for the mobile user, the network will offer the mechanism for the simultaneous uses of many users in order to widely apply for the field of actual practice. However, the method of search-address and ringing is more difficult than the common the network, for this reason, the hierarchical routing approach of WSN is able to efficiently solve the problems of complex routing, while the clustering is used for setting up and keeping the hierarchical routing.

The communicative behaviors in WSNs can be characterized by two different types: routing (node-to-sink) and broadcasting (sink-to-node or node-to-node). Broadcasting is an essential communication requirement for sink and sensor nodes. The sensor node can sense environment information and forward information to next sensor node until sink node that is named routing [5,10-12]. Therefore, how to increase stable, establish a secure network and decrease the consumption of power is an important issue.

Data aggregation is an important work for saving energy consumption whether static or dynamic WSNs. For data aggregation, certain amount of sensors in the vicinity forms a team to aggregate data [9,10]. However, WSN is made up of several clusters of sensors, and several clusters may make up of more large clusters [22]. Therefore, the topology of Cluster-based Wireless Sensor Network (CWSN) has been proposed to prolong the lifetime of WSNs by decreasing the energy consumption of SNs.

In CWSN, the topology is composed of several clusters. Each cluster is composed of many sensor nodes and one cluster manager. The sink controls the state and communication data of all cluster managers. The cluster manager controls the state and communication data of all sensor nodes. And, the sensor nodes answer to sense data. Fig. 1 is a topology of CWSN.

2.2 Byzantine Agreement Problem

In the CWSN, the sensor nodes interconnected with the wireless; the network is assumed reliable and synchronous [18]. If certain components in distributed system were failed, to achieve agreement in a distributed system the protocols are required so that systems still can be executed correctly.
The Byzantine Agreement (BA) problem [13] is one of the most fundamental problems concerning reaching agreement in distributed systems. First studied by Lamport [13], it is a well-known paradigm for achieving reliability in a distributed network of nodes. According to the definition of the BA problem by Lamport: 1) there are \( n \) nodes, of which at most \( \lfloor (n-1)/3 \rfloor \) nodes could fail without breaking down a workable network; 2) the nodes communicate with each other through message exchange in a fully connected network; 3) the message sender is always identifiable by the receiver; 4) a node is chosen as a source, and its initial value \( v_s \) is broadcasted to other nodes and itself to execute the protocol.

The solutions have defined as protocols, which achieve agreement and hope to use the minimal rounds of message exchange to obtain the maximum number of allowable faulty capability. We concern the solution of BA problem in this paper. The definition of the problem is to make the healthy nodes in \( n \)-sensor nodes CWSN to achieve agreement. The source sensor node chooses an initial value to start with, and communicates to each other by exchanging messages. The nodes of a cluster have referred to make an agreement if it satisfies the following conditions [13]:

(Agreement): All healthy sensor nodes agree on a common value.

(Validity): If the source sensor node is healthy, then all healthy sensor nodes shall agree on the initial value the source sensor node sends.

In a BA problem, many cases had based on the assumption of node failure in a fail-safe network [18]. Base on this assumption, the goal of solving a BA problem is to develop an optimal algorithm can use the minimal number of rounds to achieve an agreement.

Here we consider the network topology in a distributed system whose communication media are reliable during the BA execution in CWSN, while the node may be faulty by interference from hijackers and results in the exchanged message can exhibit arbitrary behavior. A protocol to reach agreement in a reliable communication environment of tradition network topology has proposed first by Lamport [13]. The typical protocol by Fischer [7] can tolerate \( f \leq \lfloor (n-1)/3 \rfloor \) faulty nodes in malicious and required \( \sigma = \lfloor f+1 \rfloor \) rounds(s) to get enough messages to achieve agreement.

However, most of the distributed computing systems may not be fully connected. The network topology has the feature of cluster or group just like the topology of CWSN. However, the proposed protocol MAP is used to solve the malicious sensor node fault in CWSN. When all sensor nodes achieve agreement, the fault-tolerance capacity has enhanced even if the communication media are fault between sensor nodes and the backbone can be used to provide a backup route [22].

3. The Proposed Protocol

The proposed protocol Malicious Agreement Protocol (MAP) can solve the BA problem due to faulty sensor nodes which may send wrong messages to influence the system to reach agreement in a synchronous CWSN. MAP protocol consists two phases and needs \( \sigma \) rounds of message exchange to solve the BA problem.

3.1. Protocol notation

The notations and parameters of MAP for the topology of CWSN are showed in follows:

- Let \( x, y \) be the cluster identifier where \( 1 \leq x, y \leq N \) and \( N \) is the number of clusters \( N \geq 4 \).
- Let \( f_n \) be a total number of malicious faulty sensor nodes.
- Let \( F_C \) be the maximum number of allowable faulty clusters, \( F_C \leq \lfloor (N-1)/3 \rfloor \).
- Let \( T_{F_n} \) is the total number of allowable faulty sensor nodes, \( 1 \leq f_n \leq T_{F_n} \).
- Let \( n_c \) is the number of sensor nodes in cluster \( C_x \), \( 0 \leq x \leq N \).

3.2. Protocol Model

In this section, MAP is introduced to solve agreement problems with malicious faulty sensor nodes underlying a CWSN. The proposed protocol MAP is organized as two phases, the Message Gathering Phase and Agreement Making Phase. In the Message Gathering Phase, each node is to collect enough information from other nodes in the CWSN. And, in the Agreement Making Phase, the collected information by Message Gathering Phase is used to decide the agreement value.
In the first round \((\sigma=1)\) of Message Gathering Phase, the source node sends its initial value to all sensor nodes, and then receiver node stores the received value in the root of its mg-tree. The mg-tree is a tree structure that is used to store the received message [25]. After the first round of Message Gathering Phase \((\sigma>1)\), each sensor node without source node transmits the value at level \(\sigma-1\) in its mg-tree to all nodes; At the end of each round, the receiver node takes the local majority value on the received values which are from the same cluster, to get a single value. Moreover, each receiver node stores the single value that is majority of the received values in its mg-tree.

Afterward, in the Agreement Making Phase, each node without the source node reorganizes its mg-tree into a corresponding ic-tree. The ic-tree is a tree structure that is used to store a received message without repeated cluster names [25]. Therefore, the common value \(\text{VOTE}(s)\) has obtained by using function \(\text{VOTE}\) on the root \(s\) of each node’s ic-tree. The detail steps of our proposed protocol has presented in Fig. 2.

<table>
<thead>
<tr>
<th>MAP (Source node with initial value (v_s))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definitions:</td>
</tr>
<tr>
<td>1. For the CWSN, each sensor node has the common knowledge of entire graphic information (G = (E, C)), where (C) is the set of clusters in the CWSN and (E) is a set of cluster pairs ((C_x, C_y)) indicating a communication medium (the sensing is covered) between cluster (C_x) and cluster (C_y).</td>
</tr>
<tr>
<td>2. Each sensor node can communicate with all other sensor nodes.</td>
</tr>
<tr>
<td>3. The sensor node plays sender or receiver depends on the behaviours of which kinds of transmission.</td>
</tr>
<tr>
<td>4. The sensor node cannot garble the message between the sender node and receiver node; this assumption has achieved by the technology of encryption (such as RSA [14]).</td>
</tr>
</tbody>
</table>

Pre-Execute. Computes the number of rounds required \(\sigma = \lceil (N-1)/3 \rceil + 1\), where \(N\) is the total number of clusters in the CWSN.

Message Gathering Phase:

Case \(\sigma = 1\), run

A) The source node transmits its initial value \(v_s\) to each cluster’s nodes.

B) Each receiver node obtains the value and stores it in the root of its mg-tree.

Case \(\sigma > 1\), run

A) Each node without the source node transmits the values at level \(\sigma-1\) in its mg-tree to each cluster’s nodes.

B) Each receiver node takes the local majority value on the received values from the same cluster and stores the majority single value in the corresponding vertices at level \(\sigma\) of its mg-tree.

Agreement Making Phase:

Step 1: Reorganizing the mg-tree into a corresponding ic-tree. (The vertices with repeated cluster names are deleted).

Step 2: Using function \(\text{VOTE}\) on the root \(s\) of each node’s ic-tree, then the common value \(\text{VOTE}(s)\) has obtained.

Function \(\text{VOTE}(\mu)\)

If the \(\mu\) is a leaf, then output the value \(\mu\).

Else if the majority value is not existed, then output the majority value \(\phi\).

Otherwise, output the majority \(m\), where \(m \in \{0, 1\}\)

Fig. 2. The MAP protocol

4. AN EXAMPLE BY USING MAP

In the MAP protocol, an example is given for executing our protocol MAP. An example of CWSN topology is shown in Fig. 3(a). There are 22 nodes falling into seven clusters. \(C_1\) includes source node \(n_6\) and \(n_2\). \(C_2\) includes \(n_3\), \(n_4\), \(n_5\) and \(n_{10}\). \(C_3\) includes \(n_7\), \(n_8\), \(n_9\) and \(n_{10}\). \(C_4\) includes \(n_{11}\) and \(n_{12}\). \(C_5\) includes \(n_{13}\) and \(n_{14}\). \(C_6\) includes \(n_{15}\) and \(n_{16}\), \(n_{17}\), \(n_{18}\), \(n_{19}\), \(n_{20}\) and \(n_{21}\) belong to \(C_7\).

In the BA problem, the worst situation is that the source does not honest anymore [13]. Simply, here the worst case of the example, suppose the source node \(n_s\) is malicious faulty node, which means \(n_s\) may send arbitrarily different values to
The mg-tree of healthy node $n_i$ at the second and final round in the message exchange phase is shown in Fig. 3(c) and (d), and the Message Gathering Phase has completed.

After the Message Gathering Phase, the tree structure of each healthy node has converted from mg-tree to ic-tree by deleting the vertices with duplicated names (such like $s_11$ will be deleting) in the Agreement Making Phase. The example ic-tree has showed in Fig. 3(e). Eventually, using the function VOTE to root the value $s$ for each healthy node’s ic-tree [VOTE($s_1$), ..., VOTE($s_7$) = 1], an agreement value 1 can be obtained, as shown in Fig. 3(f), and the Agreement Making Phase has completed. In the end, comparing the root $s$ value of healthy node in $C_1$, the root value of all healthy nodes in $C_1$ and $C_3$ has altered its different value to 1. In other hand, after executing the MAP protocol, all healthy nodes agree on a common value 1 for the example (Fig. 3).

Fig. 3(a). The initial status of executing MAP

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Take local majority</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma$ ($\leq 0$)</td>
<td>$s_1$</td>
<td>(0,0)</td>
</tr>
<tr>
<td>$s_2$</td>
<td>(1,1,0,0)</td>
<td></td>
</tr>
<tr>
<td>$s_3$</td>
<td>(1,0,0,0)</td>
<td></td>
</tr>
<tr>
<td>$s_4$</td>
<td>(1,1)</td>
<td></td>
</tr>
<tr>
<td>$s_5$</td>
<td>(1,1)</td>
<td></td>
</tr>
<tr>
<td>$s_6$</td>
<td>(1,1)</td>
<td></td>
</tr>
<tr>
<td>$s_7$</td>
<td>(0,1,0,1)</td>
<td></td>
</tr>
</tbody>
</table>

Fig. 3(b). The mg-tree of each node at the 1st round

Fig. 3(c). The mg-tree of healthy node $n_i$ at the 2nd round
The tree structure has converted from mg-tree to ic-tree by erasing the vertices with repeated names.

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Take local majority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>(0,0,1,0)</td>
</tr>
</tbody>
</table>

Fig. 3(d). The final mg-tree of node n after the Message Gathering Phase

- VOTE(s1) = (0, 0, 0, 1, 1, 1) = 0
- VOTE(s2) = (1, 1, 1, 1, 1, 1) = 1
- VOTE(s3) = (0, 0, 0, 0, 0, 1) = 0
- VOTE(s4) = (1, 1, 1, 1, 1, 1) = 1
- VOTE(s5) = (0, 0, 0, 0, 0, 1) = 0
- VOTE(s6) = (1, 1, 1, 1, 1, 1) = 1
- VOTE(s7) = (0, 0, 0, 0, 0, 1) = 0

VOTE(s) = (VOTE(s1), VOTE(s2), VOTE(s3), VOTE(s4), VOTE(s5), VOTE(s6), VOTE(s7)) = (0, 1, 1, 1, 1, 1, 1)

Fig. 3(e). The ic-tree of node n

Fig. 3(f). The common value VOTE(s) by healthy node n

Fig. 3. An example of MAP execution
5. **Correctness and Complexity**

The following lemmas and theorems are used to prove the correctness and complexity of protocol MAP.

### 5.1. Correctness of MAP

To prove protocol’s correctness, a vertex $\alpha$ is called common [24] if $\alpha$ of each healthy node has the same value. Thus the agreements, (Agreement) and (Validity), can be rewritten as:

(Agreement'): Root $s$ is common, and

(Validity'): $\text{VOTE}(s) = v_i$ for each healthy node, if the commander is healthy.

To prove that a vertex is common, the term common frontier [18] is defined as: When every root-to-leaf path of the mg-tree contains a common vertex, then the collection of the common vertices forms a common frontier. Based on these two terms, the correctness of MAP can be examined as follows.

**Lemma 1**: All correct vertices of an ic-tree are common.

**Proof**: After reorganization, no repeatable vertices are in an ic-tree. At the level $F_C + 1$ or above, the correct vertex $\alpha$ has at least $2F_C + 1$ children in which at least $F_C + 1$ children are correct. The true value of these $F_C + 1$ correct vertices is in common, and the majority value of vertex $\alpha$ is common. The correct vertex $\alpha$ is common in the ic-tree, if the level of $\alpha$ is less then $F_C + 1$. As a result, all correct vertices of the ic-tree are common.

**Lemma 2**: The common frontier exists in the ic-tree.

**Proof**: There are $F_C + 1$ vertices along each root-to-leaf path of an ic-tree in which the root is labeled by the source name, and the others are labeled by a sequence of cluster names. Since at most $F_C$ clusters can be failed, there are at least one vertex is correct along each root-to-leaf path of the ic-tree. By Lemma 1, the correct vertex is common, and the common frontier exists in each healthy node’s ic-tree.

**Lemma 3**: Let $\alpha$ be a vertex, $\alpha$ is common if there is a common frontier in the subtree rooted at $\alpha$.

**Proof**: If the height of $\alpha$ is 0, and the common frontier ($\alpha$ itself) exists, then $\alpha$ is common. If the height of $\alpha$ is $\sigma$, the children of $\alpha$ are all in common by using induction hypothesis with the height of the children at $\sigma - 1$, then the vertex $\alpha$ is common.

**Corollary 1**: The root is common if the common frontier exists in the ic-tree.

**Theorem 1**: The root of a healthy node’s ic-tree is common.

**Proof**: By Lemma 1, Lemma 2, Lemma 3 and Corollary 1, the theorem is proved.

**Theorem 2**: Protocol MAP solves the BA problem in a CWSN.

**Proof**: To prove the theorem, it has to show that MAP meets the constraints (Agreement’) and (Validity’).

(Agreement’): Root $s$ is common. By Theorem 1, (Agreement’) is satisfied.

(Validity’): $\text{VOTE}(s) = v$ for all healthy nodes, if the initial value of the source is $v_s$, say $v = v_s$.

Since most of nodes are healthy, they transmit the message to all others. The value of correct vertices for all healthy nodes’ mg-tree is $v$. When the mg-tree is reorganized to an ic-tree, the correct vertices still exist. As a result, each correct vertices of the ic-tree is common (Lemma 1), and its true value is $v$. By Theorem 1, this root is common. The computed value $\text{VOTE}(s) = v$ is stored in the root for all healthy nodes. (Validity’) is satisfied.

### 5.2. Complexity of MAP

The complexity of MAP is judged in terms of 1) the minimal number of rounds and 2) the maximum number of allowable faulty components.

**Theorem 3**: MAP requires $F_C + 1$ rounds to solve the BA problem with malicious fault in a CWSN where $F_C \leq \lfloor (N-1)/3 \rfloor$.

**Proof**: Due to the message passing is required in the Message Gathering Phase only. Thus, the message exchange phase is a time consuming phase. Fischer [7] pointed out that $t + 1 \leq \lfloor (n-1)/3 \rfloor$ rounds are the minimum number of rounds to get enough messages to achieve BA. The unit of Fischer [7] is node, but the unit of the CWSN is cluster. So that, the number of required rounds of message exchange in the
CWSN is $F_c + 1(F_c \leq (N-1)/3)$. Thus MAP requires $F_c + 1$ rounds and this number is the minimum.

**Theorem 4:** The total number of allowable faulty components by MAP is $F_c$ malicious faulty clusters, where $F_c \leq (N-1)/3$.

**Proof:** In Siu et al. [23] indicates the constraints of BA problem for node faults only is $f \leq (n-1)/3$. However, the unit of CWSN is cluster, so we can suppose a node in Siu et al. as a cluster in CWSN. Therefore, $f \leq (n-1)/3$ in Siu et al. imply $F_c \leq (N-1)/3$ in CWSN. So the total number of allowable faulty components by MAP is $F_c$ malicious faulty clusters.

6. **CONCLUSION**

The complex networks had studied in a branch of mathematics known as graph theory in the past. The network topology developed in recent years shows a wireless feature. The previous protocols [13,18,25] cannot adapt to solve BA problem in WSN, and none of the BA protocol is designed for the WSN. Therefore, we revisit the BA problem in CWSN with malicious faulty nodes. The proposed protocol MAP can tolerate the most damaging failure type of fallible nodes.

Actually, nodes may be crash, omission, and handoff (move in, move away or return). On other hand, the proposed protocol will be extended to consider the status (such as mobility) of nodes underlying CWSN in future work.

**ACKNOWLEDGMENT**

This work was supported in part by the Taiwan National Science Council under Grants NSC99-2221-E-324-022 and NSC100-2221-E-324-022.

**REFERENCES**


