A virtual grouping based fault-tolerant scheme for autonomous networks ☆

Jenq-Shiou Leu [a,*], Hsiao-Chuan Yueh [a], Ing-Chau Chang [b]

[a] Department of Electronic Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan
[b] Department of Computer Science and Information Engineering, National Changhua University of Education, Changhua, Taiwan

ABSTRACT

In an autonomous network environment, each independent node communicates with others by some agreement mechanism to make sure that the majority of nodes can take a common corresponding action. Under a constraint on the amount of faulty nodes, the classical solution, Byzantine Agreement (BA), has been proved to effectively make all healthy nodes able to obey the same command issued from the commander node. The major challenge for BA is its considerable amount of exchanged messages among nodes to reach the consensus, especially when BA is applied to a network environment, which comprises a lot of cooperative nodes. Such a situation may hinder BA from being practically applied in the modern network environment, such as an autonomous wireless sensor network. Thus, we propose a Virtual Grouping Byzantine Agreement (VGBA) scheme to compromise between the percentage of nodes, which can obtain the common command, and the number of exchanged messages produced in the network. That means that VGBA may suffer a lower tolerance capability of faulty nodes and a lower percentage of healthy nodes having the command, but it significantly reduces the message volume. Consequently, the improved VGBA scheme is still applicable while facing a larger number of nodes.

© 2013 Elsevier Ltd. All rights reserved.

1. Introduction

The 1980s saw a wealth of research into the properties of agreement making and how these are related to the computer system. BA (Byzantine Agreement) was first studied and defined by Lamport et al. (1982) to solve the consensus problem among cooperative nodes, such as processors in a multi-processor environment. Subsequent extensions and applications have been derived (Hsieh et al., 2010; Wada et al., 2009; Tang et al., 2009; Kate and Goldberg, 2009; Wang et al., 1995; Yin et al., 2003; Correia et al., 2004) based on the BA concept. For example, BFT (Byzantine Fault Tolerance) in (Castro and Liskov, 2002) was proposed to practically implement a fault tolerance scheme for BA. In a distributed and cooperative network environment, the BA algorithm may still be able to facilitate agreement to ensure most distributed nodes in the network autonomously reach a common value by assuming that less than one-third of the total nodes in the network malfunction. However, the major obstacle for executing

BA is the large volume of exchange messages generated when delivering the command value from the command node to other nodes on the way to reach agreement. In the past, some ideas (Kursawe, 2002; Dolev et al., 1990; Blough and Pelc, 1993; Zamsky, 1996) were proposed to optimize BA by reducing complexity of BA. In this article, we revisit the problem in which the BA protocol drives too many process cycles and an increase in the number of nodes results in a hugely increased volume of messages in the network. Even though it could guarantee a correct final result, these conditions render BA unworkable. We therefore aim to achieve a balance between the message volume and a correct result to make BA still applicable when the application can tolerate a lower degree of correctness. We propose a grouping model over the network nodes to form a two-tier BA solution – Virtual Grouping of Byzantine Agreement (VGBA) for reducing the message volume while conducting the agreement process. In this model, the message exchange to deliver the command value from the commanding node among nodes follows the Oral Message (Lamport et al., 1982) rule. A healthy node in the BA model can correctly send the received value to other nodes; whereas a faulty node is assumed to send inconsistent and arbitrary values to other nodes. The requirement for agreement in the virtual grouping based autonomous network application is that each node in the network should express its way of looking at an event and a common consensus then can be achieved based on the condition
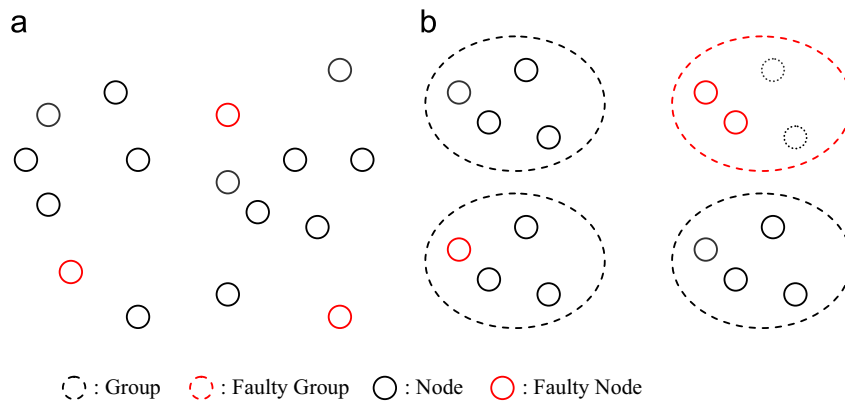
Fig. 1. An Example of Dividing Nodes by Virtual Grouping. (a) Node Distribution in the Network (16 nodes in the network) and (b) virtual Grouping (4 nodes in each group).

on each node by VGBA. Some practical examples include achieving a common opinion by referring to each member's individual perspective for a certain event in a social network or taking a common water sprinkling action by referring to each sensor node's individual sensed temperature in a sensor based fire fighting system.

Following the virtual grouping model, all nodes would first be virtually clustered in groups. If a group with h nodes has no more than $\lfloor(h-1)/3\rfloor$ faulty nodes, such a group is called a healthy group; otherwise, it is called a faulty group. For example, Fig. 1 shows a network consisted of sixteen nodes. As Fig. 1(a) shows, these nodes are uniformly virtually grouped into four groups. Three of them are healthy whereas one is faulty, as shown in Fig. 1(b). To achieve an agreement under the circumstance where some faulty nodes occur in the system, the upper bound of the faulty node volume is $\lfloor(n-1)/3\rfloor$ (n is the total number of nodes) for the tradition BA; whereas one of the faulty group volume is $\lfloor(m-1)/3\rfloor$ (m is the total number of virtual groups) for VGBA. However, this is not a precise bound of fault tolerance. We will show how to calculate the exact bound of fault tolerance in VGBA with respect to the number of nodes in Section 5.1.

The concept of our proposed VGBA is that the commander group, which contains the commander node, first executes BA to pass the command value only in the commander group. Next, our scheme proceeds to carry out a group-based BA passing the command value in the commander group to all other groups in the network, regarding each group as a node by our proposed scheme. Compared to traditional BA, the proposed scheme may have a reduced tolerance for faulty nodes, and some healthy nodes in faulty groups may not obtain the correct command value. Even though this compromised scheme cannot guarantee that all nodes will agree on a common value, it can still ensure the majority of the nodes in the network reach a consensus. Moreover, the significant reduced volume of exchange messages makes the improved BA practically applicable.

The remainder of this study is organized as follows. Section 2 depicts some past studies about BA. Section 3 introduces the basic concept of the BA protocol. Section 4 describes our proposed scheme – Virtual Grouping Byzantine Agreement (VGBA) Protocol. Section 5 illustrates the theoretical analysis and simulation results. A short conclusion is presented in Section 6.

2. Related work

BA has been used in many applications. In (Wada et al., 2009), BA is used to raise the reliability of a P2P online game by increasing fault tolerance. The authors in (Hsieh et al., 2010) applied BA to prevent the single point of failure problem from a sink in a traditional wireless sensor network environment. The local sensors can take a consistent action autonomously based on the agreement achieved by BA. Other BA based applications include secure key issuing for a P2P network (Tang et al., 2009) and distributed key generating (Kate and Goldberg, 2009).

To improve BA, the authors in Zamsky (1996) focused on reducing failure caused by faulty nodes. Two different type of failures, including a dormant fault and an arbitrary fault in a dual failure model, are discussed in Meyer and Pradhan (1991) along with a coexisting fault for the capability of fault tolerance. Furthermore, some researches have focused on optimizing the BA scheme assisted by different network models. For example, Signed Byzantine Agreement (SBA) (Hayashibara et al., 2005), a hierarchical group model, was proposed to address the issue of a large volume of messages in a P2P network environment. Meanwhile, Generalized Connected Network (Wang et al., 1995) and Grouping Byzantine Agreement (Yan and Wang, 2009) aimed to optimize the BA process over physical grouping nodes in the network. SBA encrypts the messages over the network by using a public key infrastructure (PKI). Such a PKI-based solution is costly and difficult to implement in a physical network environment. A grouping-based solution indeed facilitates the BA process. However, the physical grouping solution needs a group-oriented network (Yan and Wang, 2009) environment instead of that of the traditional BA. Our proposed scheme is based on a virtual grouping model without the need to group nodes physically. The network environment our proposed scheme faces is compatible with that of traditional BA (Lamport et al., 1982).

Another optimization approach for BA is focused on how to shorten the process time of BA (Dolev et al., 1990). With the assistance of an additional protocol, the authors in Kursawe (2002) optimized Byzantine Agreement in an optimistic way. In our proposed scheme, we do not aim to improve the original BA but rather focus on an improved message exchanging scheme in a grouping-based BA context. Therefore, our scheme – VGBA – can cooperate with the existing optimization schemes (Kursawe, 2002; Dolev et al., 1990) to achieve improved efficiency.

3. Byzantine Agreement (BA) protocol

Originally, BA (Lamport et al., 1982) has been proposed as a way to ensure all cooperative troops obey the same command from a commander through the Oral Message (Lamport et al., 1982). Gradually, the concept was applied to computer science, especially