Computer Standards & Interfaces 36 (2014) 821–830

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

The optimal generalized Byzantine Agreement in Cluster-based Wireless Sensor Networks

Shu-Ching Wang, Kuo-Qin Yan *, Chin-Ling Ho, Shun-Sheng Wang *

Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County 413, Taiwan, ROC

ARTICLE INFO

Article history:
Received 6 June 2013
Received in revised form 13 November 2013
Accepted 10 January 2014
Available online 22 January 2014

Keywords:
Wireless Sensor Network
Cluster-based Wireless Sensor Network
Byzantine Agreement
Distributed system
Internet of Things

ABSTRACT

A Wireless Sensor Network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensor nodes in a wide range of applications in various domains. In the future, WSNs are expected to be integrated into the "Internet of Things" (IoT), where sensor nodes join the Internet dynamically, and use them to collaborate and accomplish their tasks. Because of the communications of WSN will produce a broadcast storm, the Cluster-based Wireless Sensor Network (CWSN) was proposed to ameliorate the broadcast storm. However, the capability of the fault-tolerance and reliability of CWSNs must be carefully investigated and analyzed. To cope with the influence of faulty components, reaching a common agreement in the presence of faults before performing certain tasks is essential. Byzantine Agreement (BA) problem is a fundamental problem in fault-tolerant distributed systems. To enhance fault-tolerance and reliability of CWSN, the BA problem in CWSN is revisited in this paper. In this paper, a new BA protocol is proposed that adapts to the CWSN and derives its limit of allowable faulty components, while maintaining the minimum number of message exchanges.

1. Introduction

One new concept associated with the "Future Internet" is that of the so-called "Internet of Things" (IoT). The "Internet of Things" describes a vision where objects become part of the Internet, where every object is uniquely identified, and accessible to the network, its position and status known, and where services and intelligence are added to this expanded Internet, fusing the digital and physical world, ultimately impacting our professional, personal and social environments [4]. The IoT is a technological revolution that represents the future of computing and communications; its development depends on dynamic technical innovation in a number of important fields, such as wireless sensors. The purpose of the IoT consists in the facilitation of information exchanges about, among other things or goods in global supply chain networks, i.e., the IT-infrastructure should provide information about "things" in a secure and reliable manner. Extending the initial application scope, the IoT might also serve as the backbone for ubiquitous computing, enabling smart environments to recognize and identify objects, and retrieve information from the Internet to facilitate their adaptive functionality [8].

Through the study of the IoT technology, the idea of combining IoT with Wireless Sensor Network (WSN) is proposed, which demonstrates the integration feasibility of the RFID and WSN technology [4]. In order to improve the efficiency of logistics enterprises, all aspects in the transport process should be monitored, which requires applying the IoT technology into the logistics management system [10]. WSN is a wireless network consisting of spatially distributed autonomous devices using sensor nodes to monitor physical or environmental conditions cooperatively [1]. However, the sensor node is limited by the energy resource, memory, computation, communication capability, etc. [5]. Therefore, the topology of a Cluster-based Wireless Sensor Network (CWSN) has been proposed to prolong the lifetime of WSNs by decreasing the energy consumption of nodes [7].

The reliability of the node is one of the most important requirements of a successful CWSN. In order to provide a reliable environment in CWSN, a mechanism to allow a set of nodes to agree on an agreement value is required. The Byzantine Agreement (BA) problem [6,9] is one of the most fundamental problems in which an agreement value is reached in a distributed system. Some examples of such applications are the commitment problem in a distributed database system, the clock synchronization problem, and the landing task controlled by a flight path finding system [12].

The traditional BA problem first defined by Lamport et al. [9] makes the following assumptions.

(1) There are n nodes in a synchronous distributed system where n is a constant and $n \geq 4$.
(2) Each node can communicate with the others through a reliable fully connected network.
(3) One or more of the nodes might fail, so the faulty nodes may transmit incorrect message(s) to other nodes.
(4) After message exchange, all fault-free nodes should reach a

* Corresponding authors.
E-mail addresses: scwang@cyut.edu.tw (S.-C. Wang), kqyan@cyut.edu.tw (K.-Q. Yan), s10033902@cyut.edu.tw (C.-L. Ho), sswang@cyut.edu.tw (S.-S. Wang).

0920-5489/$ – see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2014.01.005

common agreement, if and only if the number of faulty nodes f_n is less than one-third of the total number of nodes in the network ($f_n \leq \lfloor (n-1)/3 \rfloor$).

(5) Only the faulty nodes are considered.

Based on these assumptions, the BA requirement can be satisfied when the following constraints are met:

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

Validity: If the source node is fault-free, then all fault-free nodes agree on the initial value sent by the source node.

Previous researches on the BA problem were solved in a well-defined network environment, such as fully connected network, broadcast network and so on [2,7,9]. In other words, all nodes reside in a wired network environment. However, the technology of networks continues to grow at a high speed and the applications in wireless mobile networks have reached an astonishing achievement level in the last year, so it is important to solve the BA problem in the wireless mobile networks. Thus, this research will focus on the wireless mobile networks and propose a protocol to make all fault-free nodes reach an agreement in the CWSN. In this study, the BA problem in CWSN is revised. The proposed protocol is referred to as the Optimal Generalized Byzantine Agreement protocol in CWSN (OGBA), which can lead to an agreement between each fault-free node in the topology of CWSN. However, the proposed protocol OGBA is the only protocol to make all fault-free nodes reach BA in the case of CWSN with both node and transmission medium (TM) fallibility.

The rest of this paper is organized as follows. Section 2 discusses the CWSN. Then, the proposed protocol OGBA is introduced and illustrated in detail in Section 3. In Section 4, an example of the execution of the proposed protocols is given. Section 5 demonstrates the fault-freeness and complexity of our new protocol. Section 6 concludes this paper.

2. Related work

The concept of the Internet of Things (IoT) was first introduced in 1999, and referred to the network connecting objects [13]. An IoT is foreseen to be a worldwide network of interconnected objects uniquely addressable, based on standard communication protocols [1]. Identified by a unique address, any object, including computers, sensors or RFID tags will be able to dynamically join the network, collaborate and cooperate efficiently to achieve different tasks. Including WSNs in such a scenario will open up new perspectives. Covering a wide application field, WSNs can play an important role by collecting surrounding context and environment information. However, deploying WSNs are configured to access the Internet raises novel challenges; these need to be tackled before taking advantage of the many benefits of such integration. The wide WSN application field can be divided into three main categories according to monitoring space, monitoring objects and monitoring interactions between objects and space [5,14]. The proposed classification can be extended by an additional category monitoring human beings.

However, when WSNs become a part of the Internet, the capability of the fault-tolerance and reliability of WSNs must be carefully investigated and analyzed. A cluster of sensor nodes in WSN is cooperating to achieve some objectives; each sensor node not only communicates with other sensor nodes by using broadcast in WSN, but also leads to a severe problem, such as broadcast storms. Therefore, the researchers proposed Cluster-based Wireless Sensor Network (CWSN) to ameliorate the broadcast storm [7]. In CWSN, each cluster is composed of many sensor nodes and one cluster head. The sink controls the state and communication data of all cluster heads. The cluster head controls the state and communication data of all sensor nodes. Fig. 1 is a topology of CWSN [4].

In the CWSN, messages are always received by receiving nodes within a fixed time period; otherwise, the message's sender is treated as a failure. If certain components in a distributed system fail, a protocol is required to ensure that the system still functions correctly. However, network components may not always work well.

In previous literature, most protocols of the BA problem perform well in wired networks [7,9,12,15]. Recent advances in technology have provided portable nodes with wireless interfaces that allow network communication among mobile users. The computing environment, which refers to mobile computing, no longer requires users to maintain a fixed and universally known position in the network, and enables almost unrestricted mobility. The topology of CWSN is a type of wireless network topology, and so previous protocols may not be well suited to it.

In a BA problem, many cases are based on the assumption of node failure in a fail-safe network [7,9]. Based on this assumption, a TM fault is treated as a node fault, whatever the correctness of an innocent node, so that an innocent node does not involve agreement [15]. Nevertheless, the definition of a BA problem requires all fault-free nodes to reach agreement.

A component is said to be fault-free if it follows protocol specifications during the execution of a protocol; otherwise, the component is said to be faulty. The symptoms of component failure can be classified into two categories: dormant faults and malicious faults [12]. Dormant faults of fallible components constitute a crash, omission, or stuck-at fault. A crash fault results when components do not work correctly. An

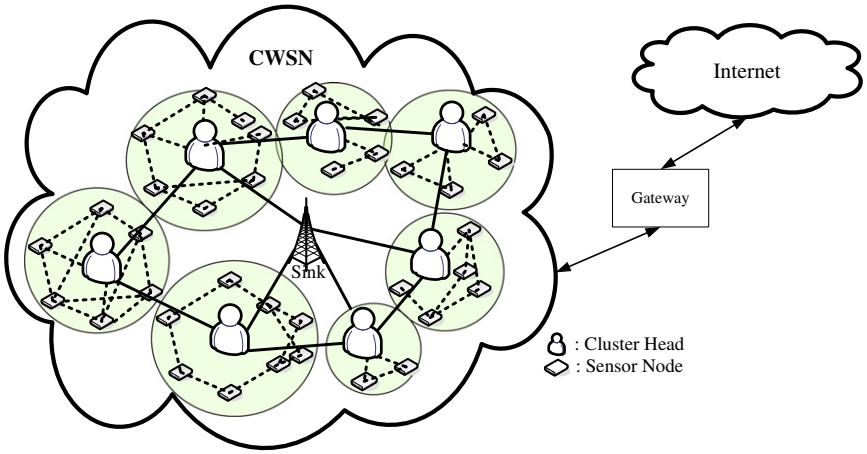

Fig. 1. The topology of CWSN.