Automation in Construction 90 (2018) 213–222

Contents lists available at ScienceDirect

Automation in Construction

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

Prototype development and test of a server-independent smart exit sign system: An algorithm, a hardware configuration, and its communication reliability

Hyunoh Kim, Ghang Lee*, Jehyun Cho

Department of Architecture and Architectural Engineering, Yonsei University, Seoul, South Korea

ARTICLE INFO

Keywords:
Evacuation guidance system
SES
Server-independent SES
Wireless sensor network (WSN)

ABSTRACT

This study introduces the first working prototype of a server-independent smart exit sign system (SISES) and validates its communication reliability. A smart exit sign system (SES) is a new type of evacuation guidance system that changes the directions of exit signs toward safe paths. Thus far, only a handful of SESs have been proposed on a conceptual level and assumed that each sign node was controlled by a central server. They are, however, complex and expensive to install and vulnerable during a fire. To overcome these limitations, an SISES, which communicates over a wireless sensor network without a central server, was proposed. This study tests the communication reliability and speed of the SISES—the most critical factors for stable operation. The results show that the SISES can communicate reliably in various conditions and that it takes less than 4 s to update the entire system installed at a 3392 m^2 building.

1. Introduction

When fire breaks out, evacuees are more likely to rely on exit signs when they are in a location that they do not know well than when they are in a familiar place [25]. Traditional exit signs show fixed directions to the nearest exit; however, this can lead evacuees into areas of greater danger if the fire has spread.

To solve this problem, a *smart exit sign system (SES)* has been proposed. A SES is a new type of evacuation guidance system with sensors that dynamically change the directions on the signs to indicate the shortest safe evacuation paths without leading evacuees into dangerous areas. Since a SES is a relatively new concept, only a few systems have been proposed thus far, even as patented ideas or algorithms [33,36,38]. The proposed systems assume the use of a central server to compute the shortest safe path from each exit sign node to the closest exit. A central server is the data server that is placed in a control room and collects fire status data directly from each sensor. Such server-based systems are simple and fast in terms of their network communication because each sensor is directly connected to a central server. They are, however, complex and expensive in terms of installation costs, and previous fire incidents have shown that a server-dependent system in general is vulnerable to a fire and can become disconnected from individual sensor nodes.

To overcome these limitations, a *server-independent (or a serverless) smart exit sign system (SISES)* has been proposed [6,12,13,15]. SISES is a special type of smart exit sign that communicates data between the exit sign nodes using a wireless sensor network (WSN) without a central server. SISES has several advantages over the previous server-dependent SESs. First, SISES is more reliable than server-dependent ones because the entire server-dependent system fails if the central server breakdowns. In contrast, the exit sign nodes in server-independent systems are not reliant on the status of the server because they do not use a server at all and can still communicate with neighboring nodes even if some nodes are damaged. The second advantage is that SISES can be installed in an existing building cost-efficiently due to no needs for wiring work and the reasonable coverage of wireless communication. If the sensor network is connected wirelessly to a central server, the more robust communication device or further bridge node to link far areas is required for covering a wide range of areas.

Despite all these advantages of SISES, only the algorithms that compute the shortest safe path with a server for SISES have been proposed independently by two research groups including the authors thus far [6,12]. The gap between a conceptual algorithm and a working prototype is, however, enormous. A hard configuration that can guarantee reliable communication in various conditions is a key requirement for any WSN-based safety system including SISES; if the individual exit sign units cannot send and receive data reliably, the entire system will malfunction. This study aims to fill in the gap between a conceptual system and a working prototype: It proposes a hardware

* Corresponding author.
E-mail address: glee@yonsei.ac.kr (G. Lee).

https://doi.org/10.1016/j.autcon.2018.02.034
Received 23 April 2017; Received in revised form 12 October 2017; Accepted 19 February 2018
Available online 14 March 2018

configuration for SISES and validates the communication reliability of the proposed hardware configuration through two sets of tests: individual factor tests and a full-scale test in a building.

By communication reliability, we mean the extent to which a system stably and consistently sends and receives data between modules under various internal and external conditions. For example, doors and walls that can potentially deteriorate the network communication are external factors, and the specifications of the network modules, such as the network packet size, are internal factors.

This paper is organized as follows. The next section reviews previous studies on fire evacuation systems and the factors that affect the communication reliability. The third section introduces a hardware configuration of SISES and an algorithm modified based on the hardware configuration. The fourth section describes the first set of validation tests—the communication reliability tests in various external and internal conditions and reports the results. The fifth section reports the results of a full-scale test in a 3392 m^2 building. The sixth section summarizes the findings and addresses the limitations and contributions.

2. Previous studies

2.1. Fire evacuation systems

Before the SES, mobile-device-based fire evacuation systems were proposed. For example, Inoue et al. [18] developed a beacon- and smartphone-based evacuation system using beacon communication and a central server to detect and provide a safe path for evacuees through a smartphone. The practicality of the system during an emergency, however, was low because the beacon-based system required an additional beacon receiver in each smartphone. Similarly, Chu et al. [8] proposed an emergency evacuation system based on radio frequency identifier (RFID) communication and a cloud server. This system assumed that evacuees would carry an RFID-enabled mobile phone and read RFID tags. The RFID tag information would be sent to a cloud server, and the cloud server would calculate and provide an updated safe evacuation route to the evacuees through their smartphones. This RFID system, however, has the same problem as the beacon-based system: the system will not work if the evacuees are not carrying an RFID reader or an RFID-enabled smartphone.

To develop a system that does not require an additional device, a research team at Yonsei University [29] developed an evacuation system based on smartphones and specially designed low-energy-consumption Wi-Fi access points, called *dummy Wi-Fis*, installed in traditional exit signs. The system does not require an additional device to receive location data and was also designed to work in blackout conditions by sharing the exit-sign battery. Nevertheless, the dummy Wi-Fi system also had limitations. In general, an indoor navigation system is composed of “fingerprints” and relies on a building map, an indoor navigation application, and the unique pattern data of Wi-Fi signals at specific locations in a building (or other types of signal patterns, such as magnetic fields, if other methods are deployed). It is unlikely that evacuees in an emergency will already have a mobile app on their phones with a map and the fingerprint data of the building; it is equally unlikely that the evacuees will download and install the data and the app during an evacuation. In addition, the system will fail if the Wi-Fi APs are broken or if the fingerprints change due to a fire.

To overcome these limitations, several researchers proposed server-based SESs that do not require a mobile device [26,30,36]. The proposed server-based SESs were designed to detect a fire using a sensor network and to guide evacuees to safe paths using a central server that would collect data from a sensor network and calculate safe paths during a fire. However, as discussed in the Introduction, these server-dependent SESs were expensive and complex to install and vulnerable to a fire. As an alternative, researchers at Imperial College London and Yonsei University (the authors) proposed a concept of and algorithms for SISES in parallel. Filippoupolitis et el. at Imperial College London proposed an algorithm that consisted of decision nodes (DNs) and mobile communication nodes (CNs) [12,13,15]. When fire breaks out, a sensor detects the fire location and then sends a message to the DNs to calculate the new path. This system has the advantage of operating with a server-independent structure. The DNs collect sensing data and compute the shortest and safest path, while the nodes share the information with their neighbors. After that, the DNs communicate the new path to the CNs—mobile devices carried by individual evacuees. The algorithm was validated through a simulation.

Similarly, Cho at el. at Yonsei University also proposed an algorithm that computes safe paths without a central server [6]. The algorithm was designed to use a WSN to collect fire detection data and to share the status information with all smart exit signs to calculate a new path. The basic approach is the same as that of the Imperial College London, but the main differences are that Cho at el. subcategorized nodes into four types (exit, plain exit sign, intersection exit sign, and dead-end exit sign) and assigned different behaviors to each node type and that the algorithm included a sub-algorithm to update the safe paths from an exit sign that detected a fire. This study also validates the applicability of the proposed algorithm through a simulation.

All these SESs, including the server-dependent and server-independent systems were, however, proposed as abstract systems, such as patented ideas or algorithms: i.e., they focused on development and validation of an algorithm and had not studied hardware and network configuration although the communication reliability of a network is a key requirement for evacuation systems based on a WSN [24]. This study focuses on the network configuration and its communication reliability of SISES. The next section reviews the factors that affect the communication reliability of a WSN before discussing the hardware configuration of SISES.

2.2. Network performance factors

This section reviews the factors that were reported to degrade the network performance in previous studies [1–5,7,10,11,14,16,17,19–23,27,28,34,35,37,39]. Publications from 2001 to 2014 were collected from three large scientific databases: IEEE.org, ScienceDirect.com, and DBpia.co.kr using the keywords WSN, WSN performance, and WSN experiment. Among numerous articles reviewed, 35 publications dealt directly with the network performance factors of WSNs. The network performance factors collected from these publications could be categorized into three groups: physical obstacles, environmental factors, and WSN properties. The following subsections describe them in detail.

2.2.1. Physical obstacles

Physical obstacles are objects that physically block communication between nodes. There are many physical obstacles in a building that can degrade the network performance of a WSN in an indoor environment [1,10,14,20,21,34]. For example, in office buildings, desk partition walls can obstruct network communication. In department stores, display stands and tables can block packet transmission. Concrete walls are the typical example of a physical obstacle. Several previous studies [1,10,20,21,34] showed that layers of a concrete walls can obstruct packet transmission. The concrete wall, however, is not a concern in SISES. This is because, in many cases by regulation, all exit signs should be located within a certain distance (15 m in the case of South Korea) of a straight line of sight, and additional exit signs should be installed at the end of all straight corridors [32]. No exit signs can, thus, theoretically and practically be blocked by concrete walls.

Fire-proof doors, however, can be a physical obstacle in SISES. Previous studies [10,14] have shown that steel doors degrade the network performance of a WSN. It has also been reported that the packet success rate decreased when two sensors were installed between at a distance of 15 m or more.

Staircases are another factor that can block packet transmission. A study shows that staircases block communication between two sensors