Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
The Journal of Systems and Software 75 (2005) 139–154
The Journal of Systems and Software
www.elsevier.com/locate/jss

Wireless protocol testing and validation supported by formal methods. A hands-on report

Manuel J. Fernández-Iglesias [a,*], Juan C. Burguillo-Rial [a], Francisco J. González-Castaño [b], Martín Llamas-Nistal [a]

[a] *Grupo de Ingeniería de Sistemas Telemáticos, Departamento de Ingeniería Telemática, Universidade de Vigo, ETSI de Telecomunicación, Campus Universitario S/N, E-36200 Vigo, Spain*

[b] *Grupo de Tecnologías de la Información, Departamento de Ingeniería Telemática, Universidade de Vigo, ETSI de Telecomunicación, Campus Universitario S/N, E-36200 Vigo, Spain*

Received 4 June 2003; received in revised form 3 February 2004; accepted 1 March 2004
Available online 12 May 2004

Abstract

We apply formal testing and validation techniques and tools to analyse a configuration protocol for a Bluetooth Location Network (BLN). This network is composed by static Bluetooth nodes that establish a spontaneous network at system initialization. Once configured, BLN provides location services for location-aware or context-driven wireless environments, such as m-commerce networks or e-museums. BLN configuration was initially defined in natural language, and had passed some initial tests and simulation-based analysis. Formal methods have provided deeper understanding and discovered unexpected errors that may arise in some failure scenarios.

Keywords: Software design; Formal testing and validation; Model checking; Wireless protocols; Bluetooth; Spin; Promela

1. Introduction

This paper discusses a case study on the application of formal methods, and more specifically Spin/Promela-based formal analysis (Holzmann, 1997, 2003), to test and validate the configuration protocol of the *Bluetooth Location Network* (BLN) described in Section 2 and in deeper detail in González-Castaño and García-Reinoso (2002). A BLN is a specialized Bluetooth (Bluetooth SIG, 2003) infrastructure composed by *static* nodes that detect *mobile* Bluetooth nodes nearby, and transmit static+mobile identifier associations to a *master* static node. Thus, the master node approximates the position of a mobile node as the location of the static node that detected it.

In a real scenario, BLN users must carry either a Bluetooth-enabled handheld, or any mobile data terminal—a WiFi-enabled PDA, a GPRS-enabled PDA, a WAP phone, etc.—*and* a Bluetooth badge. The BLN infrastructure is composed by static Bluetooth nodes, which establish an spontaneous network topology at system configuration, namely a Bluetooth *scatternet*. A scatternet consist of a network of nodes bound together by spontaneous, non-permanent links.

Bluetooth-enabled user terminals—such as iPAQ H38xx or Nokia 6310—do not require ad hoc programming for location purposes, since we rely on basic Bluetooth signaling, present at any active Bluetooth device, at the client side.

BLNs are adequate for location-aware or context-driven mobile services, such as m-commerce (Varshney et al., 2000), e-museums (Fleck et al., 2002), or electronic guidance where exhibition visitors receive specific information associated to their current location (Hsi,

* Corresponding author. Tel.: +34-986-813777; fax: +34-986-812116.
E-mail addresses: manolo@det.uvigo.es (M.J. Fernández-Iglesias), jrial@det.uvigo.es (J.C. Burguillo-Rial), javier@det.uvigo.es (F.J. González-Castaño), martin@det.uvigo.es (M. Llamas-Nistal).
URL: http://www-gist.det.uvigo.es/~manolo.

0164-1212/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2004.03.001

2002). In any of these scenarios, there may exist service providers that need to know user location in real time to send context-specific information to users' handhelds. We impose the following constraints to the location technology (BLN or other) transmitting user position to service servers:

- It must be user-independent. In other words, it must determine user position without user participation.
- The location technology must not be subject to line-of-sight constraints, due to the existence of physical barriers in museums or historical places that may prevent visitors from approaching objects. Previous research discarded automatic location-awareness for that reason (Woodruf et al., 2001).
- The location technology must be available in existing commercial handhelds as embedded network interfaces.

Many user-positioning solutions have been proposed in previous research, but they are based on specialized devices that are neither standard nor included in commercially available data terminals (Werb and Lanzl, 1998; Priyantha et al., 2000; Harter et al., 1999). If we review positioning systems supported by commercial terminals, we find the following:

- Cell phone location services (ETSI TS122071, 2003) and GPS are quite effective for outdoor applications—specially GPS, and possibly the best choice. However, they are useless indoors.
- HP's CoolTown (Kindberg and Barton, 2001) is based on IR *beacons*, which push position-dependent URLs into handheld IR ports included in most state-of-the-art PDAs and WAP phones. CoolTown is user-dependent, because the user must aim the infrared port to location beacons. It could be argued that this is a reasonable choice, since automatic detection of location information, without user participation, may have severe consequences in terms of nuisance value. CoolTown is one of the key technologies in the Electronic Guidebook Research Project (EGRP, 2003).

User-independence is not a disadvantage in educational systems, which we can expect to be less *aggressive* than e-commerce ones. Consider, for example, a museum, where updates could be associated to new halls, once the user enters them, and consist of a tiny flashing icon at the bottom of the current page meaning "do you want to update context information?" Moreover, asking the user to locate CoolTown IR beacons each time he enters a room full of visual distractions may be tiring, and signaling beacons with large red arrows unsightly. Finally, CoolTown-enabled user terminals require specialized processes for location protocol handshake.

We can conclude that, depending on each application, user-dependent line-of-sight IR systems may be more advantageous than user-independent ones or vice versa. *In fact, they are complementary*. For example, in a museum, a PDA could use CoolTown to retrieve information on a single object, and BLN-assisted context awareness to retrieve information on the surrounding hall (e.g. "Celtic *fibula*" vs. "Iron Age").

Of course, Bluetooth location nodes could be independent instead of being integrated in a network—the BLN or a wired one. In other words, each hall in a museum could have its own Bluetooth location node, which would simply push an indentifier or URL into the user terminal in a CoolTown-like fashion. However, BLN networks have two clear advantages over that approach: first, BLNs are survivable in the sense that, in case of moderate node failures, users do not suffer service denial in most cases (González-Castaño and García-Reinoso, 2003). Second, class-2 Bluetooth range does not provide enough location precision for indoor applications (Yamasaki et al., 2001), unless location nodes *collaborate* like BLN nodes do. Wiring Bluetooth location nodes is possible, but it means extra cost for no clear advantage, unless strictly necessary if a given couple of nodes cannot see each other for topological reasons, for example.

After the specification of BLN protocols in natural language, intensive simulations were performed to assess the correctness of the protocols and to evaluate their performance. As previously mentioned, a key aspect in this class of systems is survivability: BLN detection capabilities should survive in case of failures. For this, a BLN must perform a spontaneous reconfiguration when a wireless node dies, keeping as many nodes connected to the master node as possible. After a simulation-based analysis of survivability (González-Castaño and García-Reinoso, 2003), no errors were found in the protocol for typical failure patterns.

At this stage, given the positive comments of several anonymous referees, the BLN concept was thought to be mature enough to be transferred to a commercial solution. However, its designers wanted additional results showing the desired properties. They considered that, although the protocols seemed to be correct by construction, some kind of additional formal assessment was necessary. The interested reader may find similar development cycles in Burguillo-Rial et al. (2002) and Fernández-Iglesias et al. (2001).

Obviously, we can find in the literature other significant reports describing lessons learnt from real experiences (Hao et al., 2000; Holzmann, 1994; Jonkers et al., 1995; Nieh and Tavares, 1992), proposing general guidelines to assist the system engineer when considering a formal approach to design (Easterbrook and Callahan, 1997; Holloway, 1997; Holloway and Butler, 1996; Steinert and Roessler, 2000), or discussing case studies