Computers and Electrical Engineering 58 (2017) 76–87

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

MACGSP6: A protocol for supporting internet of things applications with Non-Line-of-Sight links

Maria Calle[a,*], Geovanni Berdugo[a], Juan C. Velez[a], Joseph Kabara[b]

[a] Universidad del Norte, Barranquilla, Atlantico, Colombia
[b] The TK Group, Pittsburgh, PA, USA

ARTICLE INFO

Article history:
Received 15 December 2016
Revised 5 January 2017
Accepted 9 January 2017

Keywords:
Flooding
Packet loss
Duplicate packets
NLOS
Markov Chains
Testbed

ABSTRACT

Wireless Networks with random topologies include multipath and Non-Line-of-Sight (NLOS) links, especially in urban environments. As the Internet of Things emerges many links will be NLOS. However, network protocols are often only evaluated using Line-of-Sight radio channels. Previous simulations of the MACGSP6 (Medium Access Control for Gossip-based Sleep Protocol Version 6) protocol demonstrate packet reception rates exceed 90% for networks of more than 1000 nodes with Line-of-Sight conditions. This paper measures the performance of MACGSP6 using a prototype testbed where all links are NLOS. Results demonstrate that MACGSP6 achieved better Average Packet Loss, Average Duplicate Packets and energy consumption than a controlled flooding protocol. Additionally, MACGSP6 made all degraded paths from nodes to sink appear as one ideal hop to the application layer. Therefore, MACGSP6 is an energy and data efficient protocol for Internet of Things networks which include NLOS links.

1. Introduction

Internet of Things (IoT) solutions include systems such as wireless sensor networks (WSNs), Radio Frequency Identification (RFID) infrastructure-free and infrastructure networks. The IoT includes object identification and information related to the current state of the objects like temperature, pressure, humidity, position and movement. According to the service-oriented architecture (SOA) proposed in [1], sensing and network layers of IoT may employ WSN. Possible applications for such networks include health monitoring of civil infrastructure [2] and landslide monitoring [3]. These applications require nodes to be located in strategic or random places where communication links present obstacles among different nodes; that is, links are Non-Line-of-Sight (NLOS).

Routing protocols supporting IoT networks send information through the network employing various types of overhead packets to search, create and maintain routes. Transmitting and processing overhead packets increase energy consumption, affecting battery powered nodes and network lifetime [4]. Dynamic routing protocols update routes in response to changing network conditions. Since NLOS links exhibit high packet losses [5], the network routing protocol may evaluate such link as unavailable, forcing the protocol to compute new routes, creating more overhead packets in the process. Instead, protocols for IoT networks should often transmit information even with severely degraded communication conditions. Communication protocol optimization is an ongoing research challenge in IoT [1,6]. MACGSP6 (Medium Access Control for Gossip-based Sleep Protocol Version 6) was evaluated in a testbed where all links are NLOS [5].

* Corresponding author.
E-mail address: mcalle@uninorte.edu.co (M. Calle).

http://dx.doi.org/10.1016/j.compeleceng.2017.01.008
0045-7906/

The main contributions of this paper are the following:

- Unlike other protocols, MACGSP6 was implemented in a network where all links are NLOS. Simulation results show that by employing at most two repetitions of the same information packet, MACGSP6 makes packet reception probability in a degraded network statistically indistinguishable from one ideal LOS (Line-of-Sight) hop, matching the result of an analytical model.
- Testbed links were characterized according to Received Signal Strength (RSS), and compared to Line-of-Sight (LOS) links employing the Free Space Loss Model. According to this comparison, testbed links exhibit 67.8 dB maximum signal degradation. Hence, the network creates challenging conditions for communication protocols for IoT applications.
- The hardware implementation cross-validates both analytical and simulation models.

The paper is organized as follows: Section 2 presents Related Work. Section 3 describes the hardware platform employed for the testbed. Section 4 describes MACGSP6, both algorithmically and analytically. Section 5 shows results of test performed to the platform in a linear topology, comparing them to both analytical and simulation results. Section 6 shows network tests, link characterization and MACGSP6 performance results. Section 7 concludes the paper.

2. Related work

2.1. Testbeds and prototype networks with NLOS links

Many communication protocols for WSN have been evaluated using simulations and prototype sensor platforms. Protocols such as WirelessHART (Highway Addressable Remote Transducer Protocol) have been evaluated using both simulations [7] and prototype platforms [8]. The study in [9] evaluated ZigbeePro and International Society of Automation ISA100.11a in hardware sensor nodes. Testbeds such as Twist (the TKN Wireless Indoor Sensor network Testbed) [10], Distributed Embedded Systems Testbed (DES-Testbed) [11] and MoteLab [12] employ nodes located in buildings, even on different floors. These networks include NLOS links, however, their influence is not clear since testbeds employ a large number of nodes, creating high degrees of connectivity, similar to [11]. The impact of NLOS links is more evident in a study with a prototype network using 11 MicaZ motes with 0 dBm transmission power, the Xmesh protocol and IEEE802.15.4. The test area is an outdoor environment covering a 30 m by 60 m area, with buildings and trees [13]. Results show maximum success of 48.2% when sending packets from one node to the sink. Nevertheless, these studies do not specify link distances, RSS values and NLOS conditions. On the other hand, the study in [5] characterizes links according to RSS and packet losses for analyzing performance of the Flooding protocol using a testbed where all links are NLOS. We employed the same testbed in this research.

Testbeds specifically designed for IoT experiments include SmartCampus with standard protocols such as IEEE802.15.4, Bluetooth and WiFi, deployed through an entire building [14]. A second testbed was planned to cover different buildings at the University of Padova, using IEE802.15.4 and 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) [15]. One large testbed is SmartSantander, deployed in the city of Santander, Spain, to provide smart city services and to test IoT developments as well. The testbed is organized in clusters around a gateway and, if nodes cannot communicate with it, the testbed employs repeaters [16]. The studies do not include information regarding the number of NLOS links or if they affect network performance.

2.2. Flooding and Gossip protocols

Flooding is the simplest routing algorithm where nodes must forward every received packet. The algorithm is the baseline for finding the fastest route in a network. Flooding does not explicitly create routing tables and does not generate overhead packets different than duplicates of the same data. Consequently, many routing algorithms employ variations of Flooding for information dissemination. However, Flooding produces many duplicated packets which in turn limit performance, since they increase energy consumption and traffic in the network [17].

Gossip [18] improves upon Flooding energy usage. Gossip protocols can reduce energy requirements while delivering information in IoT solutions with battery powered devices. Gossip protocols define packet forwarding according to probabilities. Therefore, information travels through the network in a similar manner to human gossip. The Gossip-based Sleep Protocol (GSP), has been implemented in simulations [19] and prototype networks [20] that cross validate each other. GSP has been extended to include both routing and Medium Access Control functions, MACGSP1 and MACGSP2 [21]. However, protocol tests included only simulations with Line-of-Sight (LOS) links.

Previous studies present Gossip protocols tested in physical networks with NLOS conditions. One study employed the DES-testbed with 111 mesh routers with IEEE 802.11 technology, located both indoor and outdoor, in three different buildings [22]. However, the DES-Testbed is designed to be an overall well connected network [11]. Another example gossip algorithm is Glossy, designed for IEEE 802.15.4 networks and tested in MoteLab, Twist and one local testbed. Glossy achieved 99% of packet delivery to nodes in the network [23]. All these examples did not explicitly report how many nodes experience NLOS conditions or the levels of obstruction between them.

MACGSP6 is a gossip protocol, tested with simulated networks including more than 1000 nodes in both random and pre-defined topologies. The protocol was compared to gossip protocols such as GSP, and to non-gossip protocols such as