Design and evaluation of a routing scheme based on drain announcements for IEEE 802.15.4 based WSNs

Carlos Lino, Carlos T. Calafate, Pietro Manzoni and Juan-Carlos Cano
Departamento de Informática de Sistemas y Computadores
Universidad Politécnica de Valencia
carlira@doctor.upv.es, {calafate, pmanzoni,jucano}@disca.upv.es

Arnoldo Díaz
División de Estudios de Posgrado e Investigación
Instituto Tecnológico de Mexicali
adiaz@itmexicali.edu.mx

Abstract

Performance, reliability and low latency are important factors in wireless sensor network (WSN) applications, especially those designed to monitor and detect time-critical events. To determine the effectiveness of WSNs based on the IEEE 802.15.4 standard at monitoring time-critical events, we develop a routing scheme based on drain announcements that seeks minimum routing overhead; this protocol is implemented on the ns-2 simulator for testing. A performance evaluation of the IEEE 802.15.4 technology under different conditions is then carried out to determine whether near real-time event monitoring is feasible. By analyzing different simulation metrics such as packet loss rate, average end-to-end delay and routing overhead, we show that the IEEE 802.15.4 standard can be used for time-critical tasks, although imposing some limitations upon the size and the amount of traffic flowing through the WSN.

1. Introduction

Given recent technological advances in wireless sensor networks, you can now develop a multitude of WSN-based applications for almost any application area, such as home, industry, environment, safety, health, target tracking, among others [1, 2].

The IEEE 802.15.4 standard [3] is the basis for the definition of the ZigBee specification [4]. ZigBee is suitable for communication with sensors, actuators and other small devices for measurement and control tasks not requiring high bandwidth, but requiring a low power consumption and a low latency. ZigBee uses the physical (PHY) and medium access control (MAC) layers defined by the IEEE 802.15.4 standard. The MAC layer plays an important role in determining the efficiency of bandwidth sharing in wireless channels and the energy cost of the communication [5].

Among the potential applications of the IEEE 802.15.4 technology we have time-critical event monitoring, in which the delivery time of recorded information is of utmost importance (e.g. fire, gas escape, and intruder detection). The main requirement imposed on WSNs when supporting time-critical event monitoring is that data must travel throughout the WSN within a short time-interval.

In this paper we introduce a routing scheme based on drain announcements that aims at minimizing routing overhead; our main purpose is that routing traffic does not to interfere with the performance measurements. The proposed routing protocol is implemented in the ns-2 simulator [6], where it is combined with IEEE 802.15.4 for testing. The performance metrics used are the packet loss ratio, the average end-to-end delay and the normalized routing load.

The paper is organized as follows: section 2 overviews some related works in this research field. Section 3 provides a brief description of the IEEE 802.15.4 standard. In section 4 we present the proposed drain announcement based routing scheme for WSNs. A performance evaluation of IEEE 802.15.4 when supporting near-real-time traffic is presented in section 5. Finally, section 6 concludes the paper.

2. Related works

In the literature we can find several works that address the behavior and performance of WSN applications. However, only a few researchers have addressed the performance of IEEE 802.15.4 when supporting time-critical event monitoring. Zheng and Lee [7], for instance, conducted a study to obtain the performance of various features such as beacon and non-beacon modes, network autoconfiguration, tree formation and association, relocation coordinator and orphans nodes for WSNs based on IEEE 802.15.4. The same authors had previously described [8] some application scenarios to show the potential of 802.15.4, including an overview of the standard and focusing on its feasibility and functionality in supporting ubiquitous networking.

In [1] authors introduce an architecture of surveillance and monitoring of mine safety, but do not specify the wireless network topology used, merely assessing the feasibility of using low-power WSN technology.

Concerning real-time WSNs, Chen et al. [9] present the tracking of multiple targets using an algorithm for multi-sensor fusion that converts the binary detection into fine positioning reports using spatial correlation. The algorithm is applied to real-time tracking of an unknown number of people moving through an outdoor field monitored by a WSN; the authors also analyze the 802.15.4 standard, both in simulation environment and analytically, determining to what degree the standard satisfies the specific requirements in real-time industrial automation. In [10] the authors describe and evaluate an architecture for real-time communication in large-scale wireless sensor networks for monitoring and control purposes. He et al. [11] present the design and analysis of VigilNet, a large-scale sensor network system which tracks, detects and classifies targets in a timely and energy-efficient manner; VigilNet is applicable in military operations, where events of interest occur at a relatively low rate, and the duration of significant events is very short.

In this paper we propose a routing protocol that proactively creates and maintains a vector field with minimum control overhead, and that enables all sensors to communicate with the drain as soon as an event is detected. Additionally, we evaluate whether the IEEE 802.15.4 is adequate for real-time tracking of critical events when operating in ad-hoc mode alone.

3. Description of IEEE 802.15.4

The IEEE 802.15.4 [3] is a standard that defines the physical and medium access control layers for wireless personal area networks with low rates of data transmission (LR-WPAN); the current version was adopted in 2006. The 802.15.4 is intended for applications that require communication with low data transmission rate and maximizing the battery lifetime. The Zigbee specification [4] builds upon the 802.15.4 standard to provide a complete solution for creating wireless sensor networks; in particular, it defines the upper levels of the protocol stack - routing and above - that the 802.15.4 standard does not cover.

The IEEE 802.15.4 standard defines the physical layer specifications (PHY) and media access control (MAC) support for devices that consume minimal power and typically operate within of a personal operating space (POS) of 10 m. Wireless links under 802.15.4 can operate in three different license-free frequency bands, known as scientific, medical, and industrial (ISM) bands. The maximum data rates supported are of 250 kbps in the 2.4 GHz band, of 40 kbps in the 915 MHz band, and of 20 kbps in the 868 MHz band. A total of 27 channels are allowed in the 802.15.4, including 16 channels in the 2.4 GHz band, 10 channels in the 915 band and one channel in the 868 MHz band.

3.1. Types of devices

The IEEE 802.15.4 standard is designed to work with two classes of devices: reduced function devices (RFDs) and full function devices (FFDs). The FFDs have the ability to communicate with any device in the network within its communication range, while RFDs are only able to communicate directly with FFDs. Each network consists of multiple FFDs and RFDs, with one of the FFDs designated as coordinator of the Personal Area Network (PAN). The FFDs can operate in three ways: *device*, *coordinator*, and *PAN coordinator*. The RFDs can operate only as *device*.

FFD devices can be used in any topology, and are capable of coordinating the network and communicating with other devices. Since RFDs can not become network coordinators, they can only communicate with a coordinator of the network, and thus a star topology is created. A device in an 802.15.4 network can use either a 64 bit address or a 16 bit short address, which is assigned during the association process. Notice that, even when relying on short addresses, an 802.15.4 network has a capacity for 65,535 devices ($2^{16}-1$), which is typically sufficient for most applications.

3.2. Network topologies

ZigBee supports three different network topologies: star, point-to-point and tree. Figure 1 illustrates these three topologies. In the star topology, the communication is established between the node devices and a central controller, called the coordinator of the Personal Area Network (PAN). The PAN coordinator can be connected to a main power supply, while the node devices are usually battery powered. Applications that can benefit from this topology include home automation, computer peripherals, toys and games. When an FFD is activated for the first time, it can establish its own network and become the PAN coordinator. In point-to-point topologies there is also a PAN coordinator. Unlike the star topology, any device can communicate with any device that is within its range, and the network can be self-organizing. The tree topology is a special case of point-to-point networks in which most of the devices are FFDs, and a RFD can connect to the network tree as a leaf node at the end of the branch. FFDs can act as a coordinators and provide synchronization to other devices and coordinators. However, only one of the coordinators can become the PAN coordinator.

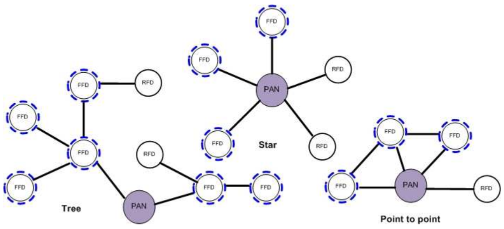

Figure 1. Networks topologies

3.3. Structure of data frames

The 802.15.4 standard defines four types of frames, including: (i) the beacon frame used by the coordinator, (ii) the data frame used for all data transfers, (iii) the receipt acknowledgment frame used to confirm successful frame reception, and (iv) the controlled MAC frame used to handle all point-to-point transfers of control of entities.

The format of an 802.15.4 data frame shown in figure 2. A MAC frame, also known as a MAC Protocol Data Unit (MPDU), consists of a MAC header (MHR), the MAC data service unit (MSDU) and the MAC footer (MFR). The first field in the header is the *frame control* field and indicates the MAC frame type that is being transmitted, the format of the address field and also controls the reception acknowledgment message. In general, we could say that it characterizes the contents of the data frame. A data frame may contain variable information about source and destination, and so the address field size can vary between 4 and 20 bytes. The payload field is also of variable length, and the maximum value of the MAC data payload field, $aMaxMACFrameSize$, is equal to $aMaxPHYPacketSize$ (127 bytes) - $aMaxFrameOverhead$ (25 bytes) = 102 bytes. The MPDU is the passed to the PHY as the PHY data frame payload, i.e., PSDU. The PSDU is prefixed with a synchronization header (SHR) and a PHY header (PHR), that together with the PSDU conform the PHY data packet, i.e., PPDU [3].

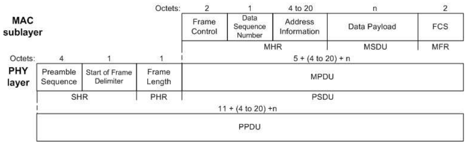

Figure 2. Data frame of IEEE 802.15.4

4. Drain announcement based routing scheme for WSNs

WSNs supporting critical event monitoring applications are characterized by stricter requirements compared to other applications. In the former the sensor nodes must react immediately upon the detection of an event and send sensed data to the drain in the shortest possible time. Notice that the relevance of data is directly related to the response time of the WSNs when, e.g., tracking an intruder. Thus, for an effective support of critical event monitoring, the time that data packets take when traveling from the sensor nodes to the drain is of utmost importance. Since end-to-end delay depends on factors such as the technology used, the routing protocol, the mean and worst-case number of hops, and the load on the network, the combined effect of these factors must be analyzed to determine the viability of a solution at supporting different critical-event monitoring applications.

To explain the drain announcement based routing scheme used, we should first mention that our target WSN environment is based on a multi-hop, single-drain scheme where sensor nodes are distributed with a density closely determined by the transmission range inherent to the IEEE 802.15.4 technology (10 meters). In the case of the drain node, this may be a fixed or mobile node with the ability to communicate and receive information sent from the different sensor nodes. The deployment of sensor nodes in these applications can be either random or manual, being that the relative location of sensor nodes is closely related to the routing protocol's performance.

Below are the major steps taken by the drain announcement based routing scheme developed for multi-node to single-drain communication:

1. The drain node is announced via broadcast messages with sequential sequence numbers.

2. Drain neighboring nodes (nodes within the transmission range of the drain) receive the drain announcement.

3. Neighboring nodes store the path towards the source node (drain), and they rebroadcast the message to all their neighboring nodes.

4. If a node receives a message containing a route towards the drain more than once, it gives preference to higher sequence numbers and, afterward, it gives preference to routes that contains the least number of hops towards the drain node.

5. Each entry in the routing table is associated with a lifetime timer, during which the route will remain valid.

6. The routes are refreshed through periodic drain announcements that are propagated to all nodes.

7. The path information is maintained in the routing table of each node until the link with neighboring nodes is lost, or until the timeout is triggered.

Algorithm 1 presents an algorithmic representation of the path discovery algorithm adopted by the drain announcement based routing scheme for WSNs that we developed.

Algorithm 1 Drain announcement message generation

```
Input: Sink_ID, interval, stop_time
Variables: packet, time, broadcast_id

BEGIN
  time = 0
  broadcast_id = 0
  REPEAT
    DrainNotify(Node_sink)
    time += interval
    Sleep(interval)
  UNTIL (time < stop_time)
END

FUNCTION DrainNotify(Node_source)
  VAR broadcast_id, request, rtable, packet
  packet.Node_source = Sink_ID
  packet.Node_dst = broadcast_addr
  packet.msg_type = DRAIN_ANNOUNCEMENT
  packet.msg_seqnum = broadcast_id++
  packet.hop_count = 0
  broadcast(packet)
END DrainNotify
```

When relying on the aforementioned routing mechanism to create and maintain routes, any sensor node willing to send or forward a report packet to the drain operates by using standard procedures: it consults its routing table to check if there is a valid path towards the drain, and then sends the information using that route; in case no route is available all traffic is discarded until a route is restored. Notice that, when doing critical-event monitoring tasks, near-real-time feedback from the networks is expected, and so buffering data for long periods of time becomes meaningless.

5. Simulation results

To assess the performance of the IEEE 802.15.4 standard in supporting time-critical WSNs we relied on the ns-2 network simulator [6]. The methodology followed for conducting the tests was the following: we implemented and validated our routing protocol for WSNs (described before) using the ns-2 network simulator. Our simulations are based on a series of repetitions, changing parameters in each set of experiments in order to achieve a holistic performance assessment of the IEEE

Table 1. Simulation parameters

Number of nodes	200
PHY/MAC	IEEE 802.15.4 / 2.4 GHz band
Traffic type	CBR
Simulation time	600 seconds
Simulation area	140x140 meters
Sensor topology	Grid
Routing protocol	Self-developed (Section 4)
Transmission range	10 meters
Packet size	50 bytes
Number of traffic sources	20
Traffic load	0.33, 1, 2, 10, 20 and 66.66 pkt/s

802.15.4 standard.

Concerning the first metric -packet loss rate- it indicates the percentage of data packets transmitted that are not received successfully, and is obtained according to equation 1.

$$Loss(\%) = \left(\frac{Number\_of\_data\_pkts\_lost}{Number\_of\_data\_pkts\_sent} \right) * 100 \tag{1}$$

Concerning the second metric -average end-to-end delay- it will allow us to know the time it takes for a message to travel from the originator sensor to the drain node, and is obtained using the following equation [12].

$$Avg\_delay = \frac{\sum_i (Reception\_t_i - Transmission\_t_i)}{Total\_data\_pkts\_received} \tag{2}$$

Finally, the third metric -normalized Routing Load (NRL)- is defined as the ratio between the number of routing packets transmitted and the number of data packets received, and is obtained using equation 3:

$$NRL = \frac{Number\_of\_control\_pkts\_sent}{Number\_of\_data\_pkts\_sent} \tag{3}$$

5.1. Set of experiments

In this set of experiments we analyze the behavior of the WSN when increasing the amount of traffic injected per source. The parameters used in these simulations are presented in table 1. We fix the number of traffic sources at 20, and increase the per-source packet injection rate basis.

Figure 3 (top) shows the performance achieved with the drain announcement based routing protocol. With respect to the packet loss ratio, it increases quite sharply for low load values, reaching about 32% loss when injecting 1 packet per second per source, for a total load of merely 8 kbit/s (notice that the maximum data rate for IEEE 802.15.4 is of 250 kbit/s when operating in the 2.4 GHz band). This occurs because each packet has to traverse several hops before the drain node is reached, with increases the chances of collision.

Figure 3 (bottom) shows the average end-to-end delay results when varying load. We can see that the average delay keeps a direct relationship with load, being that delay values become prohibitive for near real-time responsiveness (<500 ms) when sources are injecting 10 pkt/s each. For instance, in [13] the authors of SPEED, which is an adaptive real-time geographic routing protocol aiming to reduce the delay end-to-end in WSNs, the average estimated end-to-end delay is of about 300 ms for a sensor network containing 100 nodes scattered in a square area of 200x200 meters and using the 802.11 MAC layer. Notice that the minimum data rate of 802.11 is of 1 Mbit/s, four times greater than the physical data rate achieved in 802.15.4.

Concerning the routing overhead, figure 4 (top) shows the routing load for increasing traffic load. We find that the routing load is increasing slightly with traffic due to occasional malfunctioning related to congestion. However, both the total routing load and the routing load increase are within strict bounds, not representing a meaningful drawback in this context.

Figure 4 (bottom) shows the normalized

routing load for the range of packets transmitted (0.33, 1, 2, 10, 20 and 66.66 packets/second). Since traffic load is increasing drastically and routing overhead remains mostly the same, we find a steep decay which is characteristic of $\mathcal{O}(\frac{1}{n})$ function behavior.

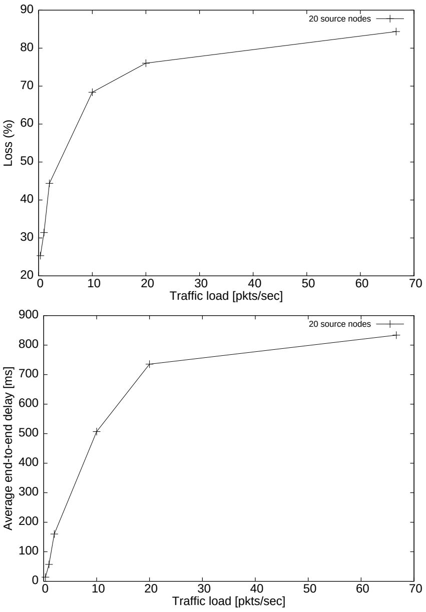

Figure 3. Packet loss ratio (top) and average end-to-end delay (bottom) when varying load.

6. Conclusions

In this paper we developed a routing protocol based on drain announcements that attempts to minimize the amount of routing traffic on the sensor network. Our main purpose was to reduce interference of control traffic upon data traffic as much as possible to maximize performance when supporting near real-time event monitoring applications.

In general, our simulation measurements showed that, despite the performance results in terms of loss rate, end-to-end delay and routing overhead were not overly satisfactory, the performance of the IEEE 802.15.4 standard was adequate to achieve reliable support for time-critical event monitoring as long as the overall packet injection rate is maintained below 20 packets per second. To support this statement the results from our set of tests show that loss and delay are extremely sensitive to the load injected per node, increasing drastically even for very low load values. Delay values experience similar growth, and the increase in terms of control traffic evidences that the network is suffers from some stability limitations.

As future work we plan to develop an enhanced routing protocol to improve the effectiveness of message delivery in the presence of mobile drains.

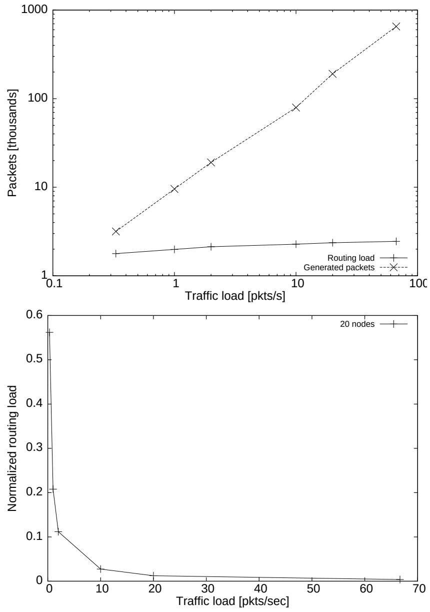

Figure 4. Number of routing/injected packets (top) and Normalized routing load (bottom) when varying the packet injection rate on a per-source basis.

Acknowledgments

This work was partially supported by the Ministerio de Educación y Ciencia, Spain, under Grant TIN2008-06441-C02-01, and by the "Ayudas complementarias para proyectos de I+D para grupos de calidad de la Generalitat Valenciana (ACOMP/2010/005)".

References

[1] A. Chehri, P. Fortier, and P. M. Tardif, "Security monitoring using wireless sensor networks," *Communication Networks and Services Research, Annual Conference on*, vol. 0, pp. 13–17, 2007.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, pp. 2292–2330, August 2008.

[3] I. C. Society, *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wirelees Personal Area Networks (WPANs)*. IEEE Computer Society, ieee std 802.15.4 2006 ed., Junio 2006.

[4] Z. Alliance, *ZigBee Document 053474r17*, January 2008. http://www.zigbee.org/ZigBeeSpecificationDownload-Request/tabid/311/Default.aspx.

[5] J. A. Gutiérrez, E. H. Callaway-Jr, and R. L. Barrett-Jr, *Low-Rate Wireless Personal Area Networks. Enabling wireless sensors with IEEE 802.15.4*. November 2003.

[6] *NS-2*. http://nsnam.isi.edu/nsnam/index.php/Main_Page.

[7] J. Zheng and M. J. Lee, "A comprehensive performance study of ieee 802.15.4," *Sensor Network Operations, IEEE Press, Wiley Interscience*, p. 14, 2006.

[8] J. Zheng and M. J. Lee, "Will ieee 802.15.4 make ubiquitous networking a reality?: a discussion on a potential low power, low bit rate standard," *Communications Magazine, IEEE*, vol. 42, pp. 140–146, June 2004.

[9] P. Chen, S. Oh, M. Manzo, B. Sinopoli, C. Sharp, K. Whitehouse, O. Tolle, J. Jeong, P. Dutta, J. Hui, S. Schaffert, S. Kim, J. Taneja, B. Zhu, T. Roosta, M. Howard, D. Culler, and S. Sastry, "Instrumenting wireless sensor networks for real-time surveillance," *Robotics and Automation, 2006. ICRA 2006. Proceedings 2006 IEEE International Conference on*, pp. 3128–3133, June 2006.

[10] C. Lu, B. M. Blum, T. F. Abdelzaher, J. A. Stankovic, and T. He, "Rap: a real-time communication architecture for large-scale wireless sensor networks," *Real-Time and Embedded Technology and Applications Symposium, 2002. Proceedings. Eighth IEEE*, pp. 55–66, January 2003.

[11] T. He, P. Vicaire, T. Yan, L. Luo, L. Gu, G. Zhou, R. Stoleru, Q. Cao, J. A. Stankovic, and T. Abdelzaher, "Achieving real-time target tracking using wireless sensor networks," December 2005.

[12] *Simulation of IEEE 802.15.4/ZigBee with Network Simulator-2 (ns-2): Performance Metrics*. http://www.ifn.et.tu-dresden.de/ marandin/ZigBee /ZigBeeSimulation.html.

[13] T. He, J. A. Stankovic, C. Lu, and T. F. Abdelzaher, "Speed: A real-time routing protocol for sensor networs," *ICDCS*, pp. 46–55, May 2003.