# AN EXPERIMENTAL STUDY OF ZIGBEE FOR BODY SENSOR NETWORKS

José Augusto Afonso<sup>1</sup>, Diogo Miguel Ferreira Taveira Gomes<sup>2</sup>, and Rui Miguel Costa Rodrigues <sup>3</sup>

<sup>1</sup> Centro Algoritmi, University of Minho, Guimarães, 4800-058, Portugal, e-mail: jose.afonso@dei.uminho.pt, phone: 351-253510184, fax: 351-253510189.

hidden node issues.

Abstract: We present an experimental performance evaluation of ZigBee networks in the context of data-intensive body sensor networks (BSNs). IEEE 802.15.4/ZigBee devices were mainly developed for use in wireless sensors network (WSN) applications; however, due to characteristics such as low power and small form factor, they are also being widely used in BSN applications, making it necessary to evaluate their suitability in this context. The delivery ratio and end-to-end delay were evaluated, under contention, for both star and tree topologies. The reliability of the ZigBee network in a star topology without hidden nodes was very good (delivery ratio close to 100%), provided the acknowledgement mechanism was enabled. On the other hand, the performance in a tree topology was degraded due to router overload and the activation of the route maintenance protocol triggered by periods of high traffic load. The effect of the devices' clock drift and hidden nodes on the reliability of the star network was modeled and validated through experimental tests. In these tests, the worst-case delivery ratio when the acknowledgment is used decreased to 90% with two sensor nodes, while for the non-acknowledged mode the result was of 13%. These results show that a mechanism for distributing the nodes' traffic over the time is required to avoid BSN performance degradation caused by router overload, clock drift and

**Keywords:** Body sensor networks, Experimental study, IEEE 802.15.4, Quality of service, Wireless sensor networks, ZigBee.

<sup>&</sup>lt;sup>2</sup> Centro Algoritmi, e-mail: a50035@alunos.uminho.pt.

<sup>&</sup>lt;sup>3</sup> Centro Algoritmi, e-mail: a50043@alunos.uminho.pt.

#### 1. INTRODUCTION

Recent advances in wireless communications, microelectronics and signal processing are enabling the development of body sensor networks (BSNs). These networks are mainly comprised by wearable or implantable sensor devices and a wireless network to transport the collected data from the users' bodies to a remote site [1]. BSNs can be used to monitor diverse physiological parameters and signals, such as temperature, heart rate, blood pressure, blood oxygen saturation, body posture, electroencephalogram (EEG), electrocardiogram (ECG) and electromyogram (EMG) [2].

BSNs can provide significant benefits in the long term diagnosis and treatments of patients, with minimum constrains to daily life activities. These networks allow the patients to move freely, inside or outside the hospital, while providing continuous monitoring, which can be particularly useful when long periods of monitoring are required. For example, many cardiac diseases are associated with episodic abnormalities, such as transient surges in blood pressure or arrhythmias [3], which cannot always be detected using conventional monitoring equipment. BSNs have the potential to provide early detection and prevention [4] of such pathologies, replacing expensive therapies later on.

IEEE 802.15.4 and ZigBee are widespread adopted network standards conceived primarily for wireless sensor networks (WSN) applications, which typically generate event based and low data rate traffic. Currently, these are also the most widely used network standards for BSNs [1],[2],[5]. However, unlike WSNs, BSNs usually generate periodic and, frequently, data-intensive traffic (e.g., ECG, EEG and body posture data). Therefore, the suitability of these standards to transport the traffic generated by this type of BSN sensors needs to be assessed.

Several works in the literature present performance evaluation results regarding IEEE 802.15.4 and/or ZigBee protocols, for different application scenarios. However, most of these results are based on analytical models [6-8] or simulations [9-10]. On the other hand, this work, which presents a revised and extended version of our previous work [11], concerns the experimental performance evaluation of ZigBee and IEEE 802.15.4 using BSN traffic. This approach provides further insight on the performance of these systems, by taking into account variables present in real-world implementations that have impact in the performance but are overlooked in most theoretical models, such as the processing load in the network nodes.

In [12], the authors present a multihop ZigBee-based BSN system for patient monitoring in hospitals, where wearable patient units using MICAz

motes are connected to a commercial blood pressure and heart rate monitor. Experimental tests in laboratory using three patient units resulted in no data loss. In [13], the authors present a multihop 802.15.4-based BSN system that measures the heart rate and blood oxygen levels of emergency room patients. The system was implemented using Telos motes and used the Collection Tree Protocol (CTP) provided by TinyOS to forward the measurements to a gateway. The measured delivery ratio was above 99.9%.

Unlike these two works, which only use low data rate sensors, our work considers sensors that generate data-intensive traffic. Three relevant quality of service (QoS) metrics are studied: delivery ratio (DR), end-to-end delay and goodput. Clock drift and hidden nodes effects were also modeled and evaluated.

#### 2. NETWORK STANDARDS AND PLATFORMS

# **2.1 IEEE 802.15.4** and **ZigBee**

The IEEE 802.15.4 standard [14] specifies the physical (PHY) and medium access control (MAC) layers for low power, low data rate and low cost wireless network devices. The PHY layer uses direct sequence spread spectrum (DSSS) and defines different transmission rates and bands: 250 kbps for the 2.4 GHz band and 20/40 kbps for 868/915 MHz band, among other possible optional configurations. The MAC layer defines two different operation modes: a non-beacon-enabled mode, which uses an unslotted CSMA-CA (Carrier Sense Multiple Access - Collision Avoidance) algorithm, and a beacon-enabled mode, which defines a superframe structure and uses a slotted CSMA-CA algorithm. The MAC layer provides also an optional guaranteed time slot (GTS) scheme, which allows the allocation of dedicated bandwidth for devices; however, this scheme is limited to a maximum of seven GTS allocations.

ZigBee [15-16] is a standard designed for low power devices used on wireless monitoring and control systems. The protocol supports star, tree and mesh topologies. In star topology, all devices communicate directly with the coordinator. Tree and mesh topologies allow to increase the range of the network by introducing routers that relay the traffic from the end devices (EDs). The ZigBee stack is based on the Open Systems Interconnection (OSI) model. Each layer performs a specific set of services for the layer above. The stack is divided into four distinct layers: physical (PHY), medium access control (MAC), network (NWK) and application (APL). The IEEE 802.15.4 standard defines the two lower layers of ZigBee: PHY and MAC. The NWK layer enables multihop network communication and is responsible to create and maintain the network, discover new routes and

assign the devices short addresses, among others tasks. The APL layer supports up to 240 applications on the same device.

## 2.2 Experimental Evaluation Platforms

The hardware platform used in the tests was the CC2530 development kit, which is provided by Texas Instruments, a leading supplier of ZigBee products. It is based on the CC2530 [17] SoC (System on Chip), which integrates a microcontroller and a transceiver in the same chip. The microcontroller is based on the 8051 architecture, and the transceiver is compliant with the IEEE 802.15.4 standard in the 2.4 GHz frequency band.

The experimental tests presented in this work were developed using the ZigBee and IEEE 802.15.4 stack implementations provided by Texas Instruments: Z-Stack and TIMAC, respectively. The Z-Stack version that was used, Z-Stack-CC2530-2.4.0-1.4.0, supports the two stack profiles of the ZigBee 2007 specification: ZigBee and ZigBee Pro. This Z-Stack version is a combination of the ZigBee stack implementation version 2.4.0 and the IEEE 802.15.4 stack implementation version 1.4.0. Some of the experiments described in this work use only the IEEE 802.15.4 stack. In these cases, the standalone TIMAC version TIMAC-CC530-1.3.1 was used.

#### 3. EVALUATON METHODS AND MODELS

This section describes the experimental evaluation methods and models that were used to obtain the results presented in the next section. Channel 26 was used, due to the absence of interference from Wi-Fi networks and other sources, verified using a spectrum analyzer. Likewise, the transmission power and placement of the nodes was set to assure that there are no packet losses due to path loss or shadowing effects, since the purpose of this study is to evaluate only the losses due to collision and transmission attempt failures of the CSMA-CA protocol caused by contention, clock drift and hidden nodes. In the tests with hidden nodes, the signals of the sensor nodes were blocked from each other using metal plates and the nodes were placed inside an anechoic chamber to avoid multipath propagation.

The default parameters of the IEEE 802.15.4 unslotted CSMA-CA algorithm were used. The overhead introduced in the data packets by all ZigBee layers accounts for a total of 264 bits, in all evaluation scenarios. All tests finish after the coordinator has received 5000 packets from the end devices. The tests presented in this work used the ZigBee Pro stack profile, but the same tests were performed using ZigBee stack and the results have shown no significant differences.

This work uses data-intensive traffic parameters extracted from a real

implementation of a body posture monitoring system composed by multiple sensor modules, each one containing three accelerometers and three magnetometers [18], which are sampled at 30 Hz. Two different traffic configurations were used. In mode A, packets are transmitted at 200 ms intervals, and the data packet length, which includes six samples from each sensor plus the protocol overhead, is 89 bytes. In mode B, smaller packets of 62 bytes with half of the samples are transmitted every 100 ms. Similar data-intensive traffic can be found in other BSN applications, such as ECG monitoring, where the sampling rate can reach 250 Hz per electrode [19].

# 3.1 Delivery Ratio and Delay

In this evaluation scenario, the delivery ratio and end-to-end delay were measured in a contention environment where multiple EDs generate packets to the coordinator simultaneously. The delivery ratio (DR) represents the ratio of the number of successfully delivered packets to the number of packets generated by the source node application. The end-to-end delay is the time since the packet is delivered for transmission by the source node application layer until it reaches the destination node application layer.

Although star topologies are more common for BSNs, multihop topologies are considered in many works [12-13]. Therefore, two topologies were evaluated: star and 2-hop tree. In the latter, a router forwards the packets from the EDs (sensor nodes) to the coordinator.

The same tests were performed with both Z-Stack and TIMAC, in order to observe the overall system behavior when supported by these two different stacks. Since the IEEE 802.15.4 standard does not define a network layer, for the tests using the TIMAC, the router of the 2-hop tree topology was simulated using a peer-to-peer network where all the EDs transmit the packets to a specific device, which relays the packets to the coordinator.

A wired trigger signal controlled by the coordinator was used to generate a periodic interrupt on the EDs according to the transmission period, which was set to 200 ms (mode A). The main objective of the trigger is to create a scenario of contention where all the EDs try to access the medium at same time, which represents a worst-case contention scenario. For the delay tests, an end device was chosen to be the reference device for the measured values.

#### 3.2 Clock Drift

This section proposes a model that uses the differential clock drift between two ZigBee end devices to estimate the duration of two parameters: the interference period ( $T_{lnt}$ ), defined as the period during which the two end devices using the unslotted CSMA-CA algorithm will contend for the channel due to the clock drift, and the interference repetition interval ( $T_{lntRep}$ ).

This model uses the times associated to a packet transmission according to the unslotted CSMS-CA algorithm of the IEEE 802.15.4 standard, which are shown in Fig. 1.

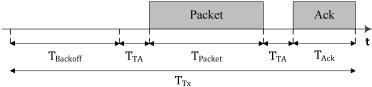


Figure 1. Times associated to the IEEE 802.15.4 unslotted CSMA-CA algorithm.

The transmission period  $(T_{Tx})$  is composed by the random backoff interval  $(T_{Backoff})$ , a transceiver turnaround time  $(T_{TA})$  from RX to TX, the packet transmission time  $(T_{Packet})$ , a turnaround time from TX to RX and, finally, the ACK transmission time  $(T_{Ack})$ . The turnaround time is defined in IEEE 802.15.4 standard and corresponds to 192  $\mu$ s. The ACK transmission time is 352  $\mu$ s, while the packet transmission time depends on the payload length.

Each end device EDn was physically connected to the coordinator (base station), to measure the number of added or missing oscillations ( $ticks_{drifted}$ ) within a period T, in comparison to the coordinator's clock. The differential clock drift between the base station (BS) and end device n can be calculated through equation 1, where  $f_{osc}$  is the nominal clock frequency of the CC2530 (32 MHz).

$$D_{BS,EDn} = \frac{ticks_{drifted}}{f_{osc} \times T} \tag{1}$$

The differential clock drift between ED1 and ED2 can be obtained, without the knowledge of the absolute clock drift of the end devices ( $D_{EDn}$ ), from the respective differential clock drifts in relation to the BS:

$$D_{ED1,ED2} = D_{BS,ED1} - D_{BS,ED2} = D_{ED2} - D_{ED1}$$
 (2)

Unsynchronized devices transmitting periodic traffic with the same nominal period will eventually contend for the wireless channel due to the clock drift effect. If the differential clock drift between ED1 and ED2 is  $D_{ED1}$ , ED2 and the nominal transmission period of the nodes is given by  $T_{ED}$ , then both nodes will start to contend for the wireless channel every  $T_{IntRep}$  seconds. The value of the interference repetition interval can be obtained through equation 3:

$$T_{IntRep} = \frac{T_{ED}}{D_{ED1,ED2}} \tag{3}$$

The interference period  $(T_{Int})$  during which two devices will compete for

the channel can be obtained through the equation 4, where  $T_{Vul}$  represents the vulnerability time window.

$$T_{Int} = \frac{T_{Vul}}{D_{ED1,ED2}} \tag{4}$$

Fig. 2 shows this vulnerability time window under which the transmissions of two nodes may interfere with each other.

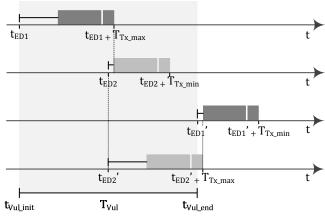


Figure 2. Vulnerability window for the clock drift evaluation scenario.

Equations 5 and 6 represent the instants of time when the interference period between devices *ED1* and *ED2* begins and ends, respectively.

$$t_{ED2} + T_{Backoff\ min} + T_{TA} = t_{ED1} + T_{Tx\ max}$$
 (5)

$$t'_{ED1} + T_{Backoff\_min} + T_{TA} = t'_{ED2} + T_{Tx\_max}$$
 (6)

 $T_{Backoff\_min}$  is the minimum backoff period, which is equal to zero.  $T_{Tx\_max}$  represents the maximum period needed to transmit a packet and receive the respective acknowledgment (if required), which is calculated using the maximum backoff period ( $T_{Backoff\_max} = 2.24$  ms).  $t_{EDn}$  and  $t'_{EDn}$  represent instants of time where device n starts the CSMA-CA algorithm. We obtain  $T_{Vul}$  from  $t'_{EDl} - t_{EDl}$ :

$$T_{Vul} = 2 \times (T_{Tx \ max} - T_{TA}) \tag{7}$$

To validate our model, we evaluated a ZigBee network formed by two end devices that transmit packets in mode B ( $T_{ED} = 100$  ms) to the coordinator in a star topology. The packet transmission time in this case is 1.984 ms. In order to better observe the interference periods and interference repetition

intervals, we forced a hidden node situation, so nodes are unable to backoff due to carrier sense, and the ACK mechanism was disabled. Therefore, in this case:

$$T_{Tx\ max} = T_{Backoff\ max} + T_{TA} + T_{packet} \tag{8}$$

## 3.3 Hidden Node Problem

In this test, two ZigBee end devices hidden from each other transmit packets in mode B in a star network topology. In order to analyze a worst-case scenario, the nodes generate packets at the same time, according to a trigger signal sent by the coordinator, and no acknowledgments are used.

The minimum transmission period ( $T_{Tx\_min}$ ) is associated to  $T_{Backoff\_min}$  (zero), while the maximum transmission period ( $T_{Tx\_max}$ ) is achieved with  $T_{Backoff\_max}$  (2.24 ms, which corresponds to 7 unit backoff periods). Given the packet transmission time in this test (1.984 ms), when the coordinator triggers a transmission in both EDs, the corresponding transmitted packets will not collide only if the transmission periods of ED1 and ED2 are equal to  $T_{Tx\_min}$  and  $T_{Tx\_max}$ , respectively, or vice versa. The probability for this specific case to occur ( $p_{TX}$ ) can be obtained through the following equation:

$$p_{TX} = 2 \times p_{Backoff\_min} \times p_{Backoff\_max}$$
 (9)

The two probabilities on the right side of this equation are equal to 1/8, since they come from a discrete uniform distribution with 8 possibilities (0 to 7). Therefore,  $p_{TX}$  is 3.125%. This value corresponds to the expected DR of the network when the ACK mechanism is not used.

## 3.4 Maximum Goodput

In this scenario a single ED transmits packets continuously to the network coordinator in the star topology. The application layer waits for the indication that the ACK has arrived before sending the next packet. The theoretical maximum goodput is obtained using equation 10, where the average transmission period is the sum of the MAC times presented on Fig. 1, using the mean backoff interval (1.12 ms).

$$Goodput = \frac{Payload\ Length\ [bits]}{Average\ Transmission\ Period\ [s]}$$
(10)

#### 4. RESULTS AND DISCUSSION

# 4.1 Delivery Ratio and Delay

During the tests with the Z-Stack in the 2-hop tree topology and with the acknowledgment mechanism enabled, a router blocking problem was observed. Through the use of a packet sniffer, it was noticed that the router relays packets for just few seconds, then blocks for around 8 seconds, after what it becomes available again and the process repeats. Several other tests were performed in other conditions, and it was verified that this problem only occurred in tests where the router was subject to high traffic load. A possible explanation for this problem is that the router experiences an overload situation where it is not able to handle packet relaying at the NWK layer when new packets are constantly being received at the MAC layer (which is a higher priority task in the Z-Stack implementation). Therefore, in order to allow the evaluation of the delivery ratio and delay during the period where the router is not blocked, the number of packets received by the coordinator for this particular experiment was reduced from 5000 to 1000 packets.

Fig. 3 presents the measured DR with Z-Stack as a function of the number of sensor nodes. For the star topology, the DR was close to 100% when the ACK mechanism was used. However, the DR for the 2-hop tree topology with 3 to 5 end devices was lower (around 96%). The explanation is that, due to the high traffic load generated by the end devices, the route maintenance protocol, triggered by the router's network layer, initiates the route discovery procedure frequently (each 5 seconds, on average). This procedure, which lasts for around 250 ms, forces the router to interrupt the packet relaying, causing packet drops due to buffer overflow. When the acknowledgments are disabled, the DR decreases significantly in both topologies as the number of sensor nodes increases, as expected.

In order to compare the TIMAC performance with Z-Stack, the length of the data packets has been equaled to the one used in the Z-Stack measurements through the introduction of dummy bytes, since the TIMAC has smaller protocol overhead. Fig. 4 presents the DR with TIMAC as a function of the number of sensor nodes.

The results with the ACK mechanism enabled are worse than the ones obtained using the Z-Stack. This is explained by the fact that the Z-Stack network layer may retransmit a packet if the MAC layer has failed to transmit it (the default is one retransmission). The non-acknowledged experiments showed better results with the Z-Stack for the tree topology, due to the router's network layer capability for buffering the received packets and relaying them in lower contention periods, whereas the application that simulates the router in the TIMAC relays the received packets immediately.

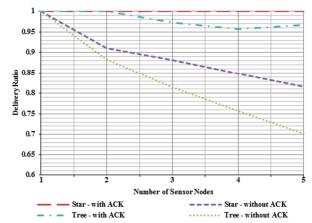


Figure 3. DR measured with Z-Stack as a function of the number of nodes.

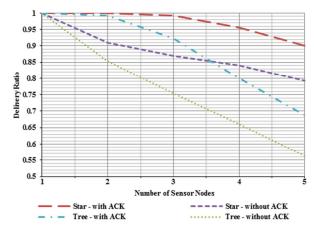


Figure 4. DR measured with TIMAC as a function of the number of nodes.

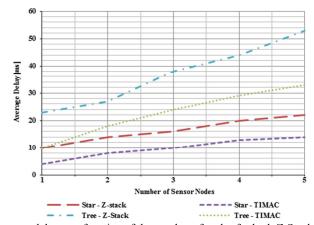


Figure 5. Average delay as a function of the number of nodes for both Z-Stack and TIMAC.

Fig. 5 and Fig. 6 show the measured average and maximum end-to-end delay, respectively, as a function of the number of sensor nodes, for both Z-Stack and TIMAC, and using the ACK mechanism. The delays measured with TIMAC are lower than those measured with the Z-Stack, due to the lower processing load introduced by the TIMAC stack. As expected, the delays increase with the number of nodes, because the contention, collisions and retransmissions also increase. The activation of the route maintenance protocol for the Z-Stack tree topology with 3 to 5 nodes causes the buffering of packets in the NWK layer, increasing significantly the maximum delay for the ZigBee network.

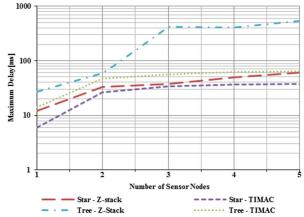


Figure 6. Maximum delay as a function of the number of nodes for both Z-Stack and TIMAC.

## 4.2 Clock Drift

Table 1 specifies the differential clock drifts between end device n and the BS ( $D_{BS,EDn}$ ).

Table 1. Measured differential clock drifts to the BS in ppm.

$D_{BS, ED\theta}$	$D_{BS, ED1}$	$D_{BS, ED2}$	$D_{BS, ED3}$	$D_{BS, ED4}$
3.6	0.1	-1.0	-0.5	0.2

We have chosen end devices 0 and 1 for the experimental measurements and model validation; for these nodes, the differential clock drift is  $D_{EDI,ED0} = 3.5$  ppm. Using these values in equation 4, we obtain a  $T_{Int}$  value of 40 minutes. The  $T_{IntRep}$  period, which can be obtained through equation 3, is 7 hours and 56 minutes. Fig. 7 shows the results obtained in this test, which uses a moving average window of 60 messages to compute the DR, corresponding to 6 seconds. The test started at 18:15:10 and ended at 13:02:44 the next day. The DR was 100% most of the time, which

corresponds to non-interference periods. The DR decreases when the interference period starts, reaches a minimum when both devices are generating packets simultaneously, and then increases again until the end of the interference period. Taking into account these boundaries, the interference period lasted for approximately 40 minutes. The interference repetition interval is approximately 7 hours and 53 minutes. The measured  $T_{Int}$  matches the value predicted by the theoretical model, whereas  $T_{IntRep}$  presents an error of 0.6%. These results validate the proposed model.

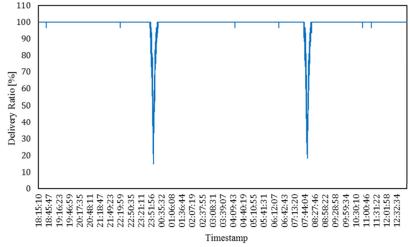


Figure 7. DR with clock drift in a star topology with two hidden nodes.

#### 4.3 Hidden Node Problem

In this evaluation scenario, the measured DR when the acknowledgment is used was 90%, whereas for the non-acknowledged mode the result was of 13%, which is very close to the minimum DR verified in the clock drift experiment, shown in Fig. 7. Previous results showed DRs in the absence of hidden nodes of 100% and 91% for two end devices transmitting in acknowledged and non-acknowledged modes, respectively (Fig. 3). Therefore, when compared with the results without hidden nodes, the results with hidden nodes show accentuated decrease in the DR. These results show that, in a scenario of contention, the DR of a simple network constituted by only two hidden EDs decreases considerably. With more hidden nodes, the network performance would be even worse. This may seriously compromise the reliability of the network and, consequently, make it unable to satisfy the QoS requirements [20] of BSN applications.

The DR measured in this experiment for the non-acknowledged mode (13%) is higher that the value predicted by the theoretical analysis (3.125%) performed on the previous section. In order to discover the origin of this

discrepancy, we analyzed the log file of this specific experiment. The theoretical analysis assumes that the coordinator should only receive packets that were sent from the nodes in the absence of collision, which is only possible if node 1 selects  $T_{Backoff\ min}$  and node 2 selects  $T_{Backoff\ max}$  when the CSMA-CA is executed, or vice-versa. Therefore, it should not be possible, in principle, to receive packets from only one of the nodes; however, this situation occurred, causing an increase on the DR. Using a packet sniffer, it was possible to observe that both nodes transmit their packets when triggered and, if one of the nodes was disabled, the coordinator receives all the packets from the other node. It was also observed that if the transmit power of the nodes were controlled in a way for the coordinator to receive equal power from both nodes, the DR decreased, while it increased if the packets were received with different power. Therefore, we conclude that the difference between theoretical and experimental results may be related with the capture effect, where, in the presence of collision, a packet may be successfully received if its power is sufficiently greater than the power of the interfering packet.

# 4.4 Maximum Goodput

Fig. 8 presents the theoretical and measured maximum goodput for star topology, as a function of the payload length, using the Z-Stack. The measured goodput is significantly lower than the theoretical values given by equation 10 because the latter was calculated using only the MAC times presented in Fig. 1. However, when the delays from the application to the MAC layer ( $T_{APP \to MAC}$ ) and vice versa ( $T_{MAC \to APP}$ ) are added to the average transmission period, the theoretical values become correct. For example, with 90-byte payload, the measured average  $T_{APP \to MAC}$  and  $T_{MAC \to APP}$  values were, respectively, 4.04 ms and 2.23 ms. Using these values, the theoretical maximum goodput becomes 59.7 kbps, which is very close to the measured value (60.5 kbps).

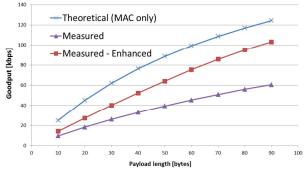


Figure 8. Maximum goodput for star topology.

A simple enhancement, which consists in sending two packets from the application layer from the MAC layer at the beginning, was implemented and tested. As shown in Fig. 8, this enhancement provides a substantial increase in the measured maximum goodput (70.7% with 90-byte payload). The rationale is that the MAC layer will always have a spare packet available on its buffer and therefore it can bypass most of the delay between the application and MAC layers.

#### 5. CONCLUSION

This work presented an experimental performance analysis of ZigBee in the context of the BSNs, using the Texas Instruments implementations of ZigBee (Z-Stack) and IEEE 802.15.4 (TIMAC).

For 2-hop tree, tests have shown that successive periods of high traffic load can cause the ZigBee router to start the route discovery procedure, with negative impact on the delay and DR. A router blocking problem, which is also caused by high traffic loads and lasts several seconds, was also observed.

Results from the clock drift analysis showed that interference periods may last for a long time due to the small clock drifts between nodes. The experiments have also demonstrated the validity of the proposed clock drift model, where the theoretical and experimental results are close.

Other results have shown that the DR with hidden nodes is considerably worse. Although this experiment considered a worst-case contention scenario, due to the synchronization of packet generation instants, only two end devices were used. Multiple hidden nodes combined with the clock drift effect may cause frequent network reliability problems during long periods.

Since BSN applications demand specific QoS requirements, these results suggest that it is necessary to provide a mechanism to distribute the traffic load generated by high traffic nodes along the time in ZigBee-based BSNs, in order to prevent the router overload, clock drift and hidden node issues.

# **ACKNOWLEDGMENT**

This work is funded by FEDER funds through "Programa Operacional Fatores de Competitividade – COMPETE" and by National Funds through FCT – Portuguese Foundation for Science and Technology in the scope of the Project FCOMP-01-0124-FEDER-022674.

#### REFERENCES

- 1. M. Chen, S. Gonzalez, A. Vasilakos, H. Cao and V. C. M. Leung, Body area networks: A survey, Mobile Networks and Applications, 16(2), 2011, pp171–193
- A. Pantelopoulos and N. Bourbakis, A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 40(1), January 2010, pp1-12
- B. Lo and G. Z. Yang, Key technical challenges and current implementations of body sensor networks, Proceedings of BSN 2005, April 2005, London, UK.
- A. Chen et al., HDPS: Heart Disease Prediction System, Computing in Cardiology, 38, 2011, pp557-560
- H. Yan, H. Huo, Y. Xu and M Gidlund, Wireless Sensor Network Based E-Health System –Implementation and Experimental Results, IEEE Transactions on Consumer Electronics, 56(4), November 2010, pp2288-2295
- Z. Chen, C. Lin, H. Wen and H. Yin, An analytical model for evaluating IEEE 802.15.4 CSMA/CA protocol in low-rate wireless application, Proceedings of AINAW 2007, May 2007, Ontario, Canada, pp899-904
- X. Liang and I. Balasingham, Performance Analysis of the IEEE 802.15.4 based ECG Monitoring Network Proceedings of Seventh IASTED International Conferences Wireless and Optical Communications, June 2007, Montreal, Canada, pp99-104
- 8. J. S. Choi and M. C. Zhou, Performance analysis of ZigBee-based body sensor networks, Proceedings of IEEE SMC 2010, Istanbul, Turkey, pp2427-2433
- J. Zheng and M. J. Lee, A Comprehensive Performance Study of IEEE 802.15.4, Sensor networks operation, 4, 2006, pp1-14.
- G. Lu, B. Krishnamachari and C. S. Raghavendra, Performance Evaluation of the IEEE 802.15. 4 MAC for Low-Rate Low-Power Wireless Networks, Proceedings of IEEE IPCCC 2004, April, Phoenix, USA, pp701-706
- D. Gomes, C. Gonçalves and J. A. Afonso, Performance Evaluation of ZigBee Protocol for High Data Rate Body Sensor Networks, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering 2013, WCE 2013, 3-5 July, 2013, London, U.K., pp1468-1473
- 12. A. Hande, T. Polk, W. Walker and D. Bhatia, Self-Powered Wireless Sensor Networks for Remote Patient Monitoring in Hospitals, Sensors, vol. 6(9), pp. 1102-1117, 2006.
- 13. J. Ko, T. Gao and A. Terzis, Empirical Study of a Medical Sensor Application in an Urban Emergency Department, Proceedings of BodyNets '09, Los Angeles, USA
- IEEE Std 802.15.4-200, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), September 2006
- 15. ZigBee Standards Organization, ZigBee Specification, Document 053474r17, January 2008
- 16. D. Gislason, Zigbee Wireless Networking, Newnes, 2008
- 17. Texas Instruments, A True System-on-Chip Solution for 2.4-GHz IEEE 802.15.4 and ZigBee Applications, CC2530 datasheet, February 2011
- J. A. Afonso, J. H. Correia, H. R. Silva, L. A. Rocha, Body Kinetics Monitoring System, International Patent WO/2008/018810, February 2008
- M. Paksuniemi, H. Sorvoja, E. Alasaarela and R. Myllylä, Wireless sensor and data transmission needs and technologies for patient monitoring in the operating room and intensive care unit, Proceedings of 27th IEEE EMBC, September 2005, Shanghai, China
- H. F. López, J. A. Afonso, J. H. Correia and R. Simões, The Need for Standardized Tests to Evaluate the Reliability of Data Transport in Wireless Medical Systems, Lecture Notes of ICST, 102, June 2012, pp137–145