A STUDY OF QOS 6LOWPAN FOR THE INTERNET OF THINGS

Nejikouka[1] and Adel Thalajoui[2]

[1]ISITCOM, University of Sousse, Tunisia
[2]University of Toulouse-UT2, CNRS-IRIT-IRT, France

ABSTRACT

6LowPAN was introduced by the IETF as a standard protocol to interconnect tiny and constrained devices across IPv6 clouds. 6LowPAN supports a QoS feature based on two priority bits. So far, little interest has been granted and this QoS feature and there are no implementations of such feature in real networks. In this paper,we evaluate the capacity to provide QoS of these priority bits in various scenarios. We show that under very heavy or very low network load, these bits have a limited effect on the delay.

KEYWORDS

Internet of Things, 6LowPAN, QoS, TF.

1. INTRODUCTION

An Internet of Things (IoT) system connects the physical world into Internet via radio frequency identification (RFID) tags, sensors, and mobile devices. 6Lowpan(IPv6 over Low-Power Wireless Personal Area Networks) is a promising IoT IETF standard for connecting sensors across IPv6 clouds. Some sensing applications are time sensitive and may require bounded delay in sending the sensed data. In particular, military, mission critical and safety domains generally require rapid and/or real time data transfer.

Therefore, some QoS feature would be required to give sensor network administrators the ability to control the overall network performance. 6LowPAN offers a QoS feature based on two priority bits. So far, no implementation of these priority bits was done. In this paper, using simulation, we evaluate the effectiveness of these priority bits in various scenarios. We show that under very heavy or very low network loads, these bits have a limited effect on the delay. However, in most realistic cenarios where the network is reasonably loaded (between 40 to 80 %), it is straight forward to apply a priority-based QzoS priority in 6Lowpan. The remainder of this paper is organized as follows. In Section 2, we describe some related work primarily in classical IP networks. In Section 3, we describe the QoS features of 6LoWPAN. Simulation results are presented in Section 4 and we finally draw the conclusions in Section 5.

2. RELATED WORKS

There are two application classes: throughput and delay tolerant elastic traffic and the bandwidth and delay sensitive inelastic (real-time) traffic.

DOI: 10.5121/ijcacs.2016.1301

RFC 2368 [1] definition on Internet QoS. IntServ model and DiffServ model [2, 3] are the typical QoS models employed in the Internet, which employs reservation-based and reservation-less approach, respectively. In other words, the QoS solutions such as IntServ and DiffServ developed for traditional networks cannot be easily ported in WSN and internet of things due to severe resource constraints in sensor nodes, large-scale and random deployment of sensors and applications specifics in WSN. The two perspectives of QoS in WSNs described in [4], namely application-specific QoS and network QoS, represent the two major categories of the existing research for WSN QoS.

3. QOS FOR IOT

In this section we interested with the QoS for each layer, we focus in priority as part of QoS.

3.1 QOS AT PHSYSICAL LAYER

The IEEE 802.15.4 [5] defines low-power wireless Embedded radio communications at2.4GHz, 915 MHz and 868 MHz. In practice IEEE 802.15.4 at 2.4 GHz is used almost exclusively today as it provides reasonable data rates, and can be used globally. IEEE 802.15.4 specification defines the physical and link layer of the IoT and WSN. The 802.15.4 standard provides 20-250 kbit/s data rates depending on the frequency. Channel sharing is achieved using carrier sense multiple access (CSMA), and acknowledgments areprovided for reliability. This standard supports three types of topologies: star, tree and mesh. Each IEEE 802.15.4 network has a special node dubbed network coordinator, which defines a set of characteristics of the network such as addressing, supported channels, and operation mode.The network can operate either in a beacon enabled mode or in a nonbeacon-enabled mode.

In the beaconless mode, the Protocol is essentially a simple Carrier Sense Multiple Access with Collision avoidance (CSMA-CA) protocol. Since most of the unique features of IEEE 802.15.4 are in the beacon-enabled mode, like support for communications with real-time restrictions we will focus our attention on this mode. In the beacon enabled mode the network coordinator coordinates the access to the network by periodically transmitting a special frame dubbed Beacon, which delimits the structure dubbed superframe that specifies the intrinsic rules to perform such access. The period that specifies the consecutive beacon transmissions is dubbed beacon interval (BI).may comprise two periods: a mandatory active period, and an optional inactive period. Each active period is divided into a contention access period (CAP), and an optional contention free period (CFP).

The CAP was designed for general purpose traffic, using a contention-based approach in the access of the network. Divided in transmission windows dubbed guar-anteed time slots (GTSs) that Uses an Exclusive and contention-free approach in the access of the network. Once a given GTS slot is allocated to a node, only this node can transmit in this time interval. Finally, the inactive period was designed to power-saving purposes, where all nodes use such period to save the energy spent in the listen process.

3.1.1. QOS FOR THE STACK :ZIGBEE/802.15.4

One of the key decisions for the development of Internet of Things is the architecture and protocols used. In follows we will present a state of the art of quality of service for the protocol

802.15.4. The density of the nodes and algorithms developed must have a very good scalinefactor : it is the first difference with WLAN how has a number of stations generally does not exceed one hundred.

We will address the issue of providing quality service to the IEEE 802.15.4 and ZigBee because there completely stack and we cantseparte it. The MAC can be run in two modes: beaconless mode and beacon-enabled mode. Beaconless mode uses pure CSMA channel access and Beacon-enabled mode uses a hybrid time division multiple access (TDMA) approach, with the possibility of reserving time-slots for critical data.

Link-layer security is provided with 128-bit AES encryption. Addressing modes for 64-bit (long) and 16-bit (short) addresses are provided with unicast and broadcast capabilities. The physical layer payload is up to 127 bytes.

ZigBee / 802.15.4 is an interesting choice for the Internet of Things. It provides a communication wireless coupled with low cost and low energy consumption.

The ZigBee protocol stack defines the network and application layers above the physical and link layers standardized by the IEEE 802.15.4. Indeed ZigBee specification proposes a protocol stack owner and lightweight. Available in several versions. It relies on IEEE 802.15.4 (IEEE. 2003). It offers its own upper layers (network, etc. .) and although ZigBee achieves high energy savings through optimization periods of standby equipment (Freescale , 2005).

So, 802.15.4 implements a deterministic media access at the data link layer for applications requiring time guarantees mechanism . The warranty is limited to the one-hop communication which is insufficient for multi-hop networks such as like used by ZigBee. Several studies have been made for optimized access to the wireless medium.

A. QOS MODEL FOR SINGLE-HOP

In the model of single-hop communication, the transmitter can reach the receiver directly. An example is the deployment of the star topology, or all nodes only communicate with the central node. The support of the quality of service in such a network is set in the MAC sublayer of the data link layer . For the IEEE 802.15.4 standard , improvements were recorded for two channel access mechanisms : the CSMA/CA for shared access and GTS mechanism for deterministic access .

For the CSMA / CA protocol , offering quality service is based on the addition of priorities to messages according to their urgency, either by modifying the protocol parameters according to these priorities , or by limiting the competition for access channel nodes with priority messages. Regarding the GTS mechanism, which already has deterministic time guarantees transmission, its main fault was limited the maximum number of nodes that can allocate " slots time". This problem was resolved with sharring of aslot.

B. QOS MODEL FOR MULTI-HOP

Providing quality of service in the single data link layer is insufficient. The QoS mechanisms must be included in the network layer to have end-to- end guarantees.

These mechanisms are put inthe routing protocols. The SPEED protocol is classified as geographic routing protocols, based on the quality of service. Its key feature is a guaranteed delivery of optimal end to end communications for sensor networks. With this specification, SPEED is the most appropriate protocol for real-time applications, generally the Internet of Things .Indeed , this protocol and tries to achieve a constant transmission rate of packets throughout the network .

To ensure the quality of routing with real-time service SPEED interworking of several modules. Inspired by the previous protocol, the protocol MMSPEED has a change in protocols with QoS.

More benefits inherited from the SPEED protocol, MMSPEED is characterized by the provision of multi-speed transmission and the possibility of establishing more than a path to the destination. Indeed, each speed offered to define a level of temporal QoS and each additional road helps improve the quality of traffic. These two mechanisms allow respectively to observe the degree of criticality of each application, to forward packets within the required time, avoid common problems such as congestion and reduce the rate of packet loss. So the MMSPEED differs by offering multiple levels of QoS according to the requirements of traffic. PRAR is a routing protocol which is said to be soft real-time : It tries to ensure timely communication. required by applications while consuming less energy. It is based on the following hypothesis: the more energy , the less transmission time limit . Thus, the protocol establishes a compromise between the energy consumption and time transmissions.

3.2. QoS AT LINK-LAYER

In the following paragraphs, a summary of current QoS MAC solutions for IoTs is provided. Two complete surveys of QoS-Aware MAC protocols and Real Time (RT) QoS support can be found in [6] and [7] respectively. This section below describe the smajor differences of protocols used to support QoS.

1) IEEE 802.15.4 standard [8]: it basically uses CSMA/CA in the beacon-enabled synchronized mode, and provides guaranteed time slots (GTS) in the Implicit prioritized access protocol

IEEE 802.15.4 physical layer and MAC layer standard for low-rate personal area networks has de facto established as the most suitable, but still not optimal standard for WSN applications.

2) PEDAMACS [9]: this TDMA-based protocol that aims to achieve both energy efficiency and delay guarantee (HRT).

3)(I-EDF) [10] and dual-mode MAC protocol [11]: they adopt a cellular backbone network and thus they are topology-dependent. They use Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA) to guarantee bounded delay (HRT).

4) Saxena et al. [12]: the autors propose a CSMA/CA protocol designed to support three types of traffic: streaming video, non-real-time and best effort. The device adjusts the duty cycle depending on the dominating traffic received in order to achieve energy saving.

5) PQ-MAC [13]: it uses both CSMA and TDMA. Energy saving is handled by an advanced wake up scheme, while prioritization is handled by a doubling scheme for high priority data.

6) I-MAC [14]: this protocol is based on Z-MAC [15] and defines three priority levels. It uses both CSMA and TDMA.

7) Diff-MAC [16]: it is a CSMA/CA based protocol, which provides differentiated services and hybrid prioritization very useful in multimedia applications. Its dynamic adaptation brings higher complexity.

3.3. QoS AT NETWROK LAYER

At the network layer, we focus in 6lowpan [17] and we show the impact of the packet compression and fragmentation on QoS. In addition, we discus priority on TF field on QoS.

3.3.1 IPv6 AND 6LOWPAN

A. QoS FOR IPv6

The use of IPv6 for the IoT has several advantages including easy and self-configuration of objects, of course he solved the problem of shortage of IPv4 addresses. QoS for IPv6 is based on Traffic Class and Flow Label. The Traffic Class (TC) field in the IPv6 header comprises 6 bits of Diffserv extension [RFC2474] and 2 bits of Explicit Congestion Notification (ECN) [RFC3168].The 20-bit flow label field in IPv6 packet header provides used for packet marking, flow identification, and flow state lookup. RFC 3697 [28] describes the specification.

B. QoS FOR 6LOWPAN

The contrast between the size of 802.15.4 packet and the fact that the MTU of IPv6 is 1280 bytes, leads to the need of fragmentation and header compression to carry IPv6 packets over the packet 802.15.4. 6lowpan adaptation layer is between the network layer and the link layer. It receives from the network layer IPv6 packets of 1280 bytes (minimum MTU) and sends it to its equivalent on the remote device in 802.15.4 frames. The 6lowpan packets are transported by 802.15.4 packet as payload. They are components of a fragment header, IPv6 header compressed (6lowpan) and a byte called "dispatch" always precedes these attributes and defines their properties.

RFC 4919 and 4944 defines the compression mechanism of the IPv6 headers to LoWPAN. It also defines the compression of the UDP header of 8 bytes values of 4 bytes.

This RFC describes two types of compression: compression of IPv6 header (HC1) and the transport header compression or compression (HC2). HC1 describes how compressed IPv6 header of 40 bytes to 3 in the best case and HC2 sets the compression transport layer or UDP, as ICMP and TCP will not be compressed.

The first version of 6lowpan designed for local communication. In order to solve local and global addresses, RFC 6282 define new compression header called LOWPAN_IPHC. This 40-byte header size is reduced by 2 bytes for local addresses : dispatch and LOWPAN_IPHC. When routing over multiple hops, LOWPAN_IPHC can compress the IPv6 header down to 7 bytes :1 byte dispatch, 1 byte LOWPAN_IPHC, 1 byte Hop Limit, 2 byte Source Address and 2 byte Destination Address.

The TF bits control how the IPv6 header fields traffic class and flow label are handled as the flow label is an unstructured 20-bit label [RFC 2460, RFC 3697], provision is only made to completely elide it if all bits are zero (the value for packets that are not part of any specific flow). The assumption is that ECN and differentiated services can be put to good use in resource-constrained LoWPANs. The three (sub) fields can be sent essentially unchanged (slightly reordered so that ECN is always sent first if sent at all, TF = 00), the DSCP part of the traffic class can be elided if all bits are zero (TF = 01), the flow label can be elided if all of its bits are zero (TF = 10), or both traffic class and flow label can be completely elided if they are both entirely zero (TF = 11).

3.4. QoS at Transport layer

3.4.1 HC2 and LOWPAN_NHC compression

RFC 4944 defines the compression of UDP header or HC2. The HC2 byte defines the compression format of the UDP header . With 6lowpan compression, HC2 follow HC1.The UDP format (8 bytes) is compressed to 4 bytes : HC2 + 3 bytes of header compression.RFC 6282 also defines the compression of next headers.

Therefore in the likely best case the 6LoWPAN/UDP header is just 6 bytes in length. By comparison a standard IPv6/UDP header is 48 bytes in length .Comparatively, ZigBee has a seven-byte header for communicating over a single hop and a 15-byte header when communicating over multiple hops, which is equal or larger to 6LoWPAN's compressed UDP/IPv6 header .So we benefit 87.5% of header length, this benefits of compression headers decrease delay and use efficient channel

3.4.2 TCP for IoT : QoS problems

Connection setup : TCP is connection oriented and each session begins with a connection setupprocedure. This is unnecessary, given that most of the communications within the IoT will involve the exchange of a small amount of data and, the setup phase would last for a considerable portion of the session time.

Congestion control : TCP is responsible of performing end -to-end congestion control. In the IoT this may cause performance problems as most of the communications will exploit the wireless medium, which is known to be a challenging environment for TCP]. Furthermore, if the amount of data to be exchanged in a single session is very small, TCP congestion control is useless, given that the whole TCP session will be concluded with the transmission of the first segment and the consequent reception of the corresponding acknowledgement.

Data buffering : TCP requires data to be stored in a memory buffer both at the source and at thedestination. Management of such buffers may be too costly in terms of required energy for battery-less devices.

Reliability : Standard Internet protocols are not optimized for low-power wireless networks. Forexample, TCP is not able to distinguish between packets dropped because of congestion or packets lost on wireless links.

3.5 QOS AT APPLICATION LAYER

3.5.1 STACK COAP / UDP VS HTTP / TCP

The HTTP protocol is a way to implement architecture for access to objects, but this protocol is very intensive for resource. It is based on TCP, the most transport protocol used on the Internet. This allows more reliable transmissions by detecting transmission errors and retransmitting lost packets and also to implement flow control to adapt the transmission rate to the network capacity.

The format of the HTTP headers is relatively great, which enables greater scalability, however their treatment also requires significant resources. The CoAP protocol [18], allows to removing HTTP limitations while ensuring a high level of compatibility with the existing. CoAP consider these caches as databases where information may be stored during their period of validity. An even bigger benefit of CoAPvs HTTP for LLNs is the simplified transaction. Retrieving the representation of a resource on a CoAP server is as simple as sending the GET request and retrieving the ACK, with the data piggy backed in return.

4. SIMULATION RESULTS

In this simulation we evaluate the influence of priority in QoS6lowpan. We use in this simulation omnet++, contiki [19].

4.1 Architectures of simulations

We chose a network infrastructure as follows in Fig1.

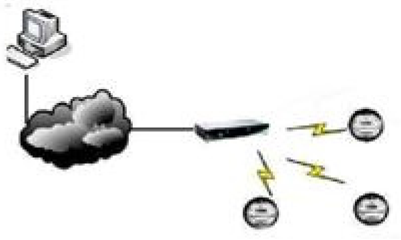


Figure 1. Example of proposed composite network

Infrastructure, because the routing is not study in this paper we evaluate QoS with a single hop.
This table show parametrs for simulation

Tab 1 : characteristics of simulation

Parametr	Value
Application	UDP , Ping
Network Layer	IPv6/6LoWPAN
MAC/PHY	IEEE 802.15.4 (CSMA-CA)
Radio duty Cycling Algorithm	Null radio duty cycling
Propagation Loss Model	FriisPropagationLossMoDel
Maximum Bit rate	250 kbps

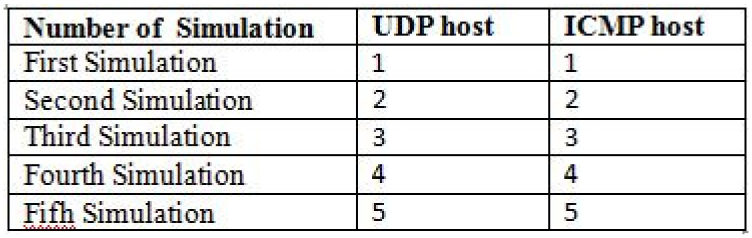
The infrastruture network is composed by :

*N nombre hosts of wireless 6lowpan/802.15.4 network applications, which are converse with other wired host using 6lowpan and ethernet protocol.
*Node how generating UDP streams with a rate of 16 kbit/s (asreprsent a priority trafic).
Node how generating Ping streams with a rate of 8 Kbit/s(as represent a no priority trafic).

*A node acts as gateway. Generally, in existing networks, the different streams converge towards the same point as a hybrid router.

* Router 802.15.4 is the link between 6Lowpan/802.15.4 and UDP/IPv6/Ethernet stack.
*A node playing the role of Wired host.

We begin with one host UDP and one host ICMP and after that for each time we add a new host for the both traffic and we show the impact on end to end delay. Our idea is how to show the impact of priority vsincresing of flow. The number of host for each case of simulation is shown below



Number of Simulation	UDP host	ICMP host
First Simulation	1	1
Second Simulation	2	2
Third Simulation	3	3
Fourth Simulation	4	4
Fifh Simulation	5	5

Table 2.Scenarios of simulation

These scenarios are tested with and without use of field TF.For the case without TF the script under contiki, sicslowpan.c is modified with the goal is to ommeted TF for this simulation

4.2. End to end delay

4.2.1. With and without priority (UDP)

In Fig.2 it is showed the end-to-end delay time (in ms) for a 6LoWPAN communication in a network with 1 hops and an application data payload ranging from 2 to 10 nodes. Nodes were at a constant distance of 20 cm from each other. The value of the 5 observation is the resulting end-to-end delay time as shown in Fig2.

It can be explained the difference between end-to-end delay obtained for the case with and without TF for UDP traffic, the first one has important values the case of without TF, with a peak of 2.1ms for the booth case.

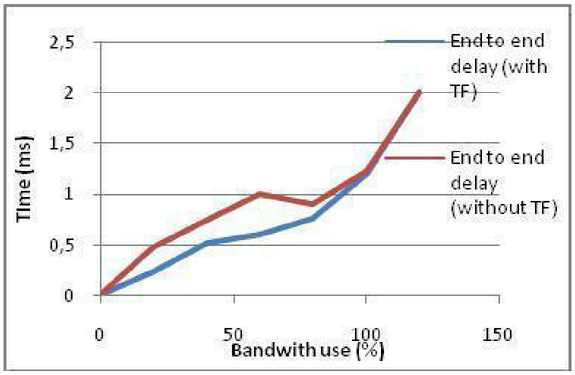


Figure 2. End to end delay with TF

First the QoS for the scenarios with field TF is set when we have a little traffic (Between 0 and 90 %). After that, the TFis obsolete indeed there are same mean end to end delay.

So with the result we conclude that TF has a importance when the number of urgent traffic are less. En fact between 0 and 90% the use of TF in lowpanamelioreQoS but when they traffic became great the priority has not meaning.

4.2.2 With and without priority (Ping)

Fig 3 demonstrates the mean end to end delay for Ping application with and without use of TF.

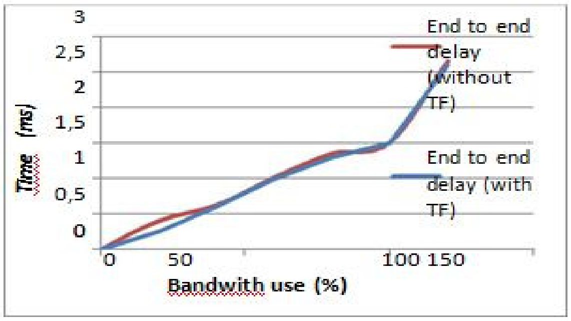


Figure 3. End to end delay without TF

For this scenario, the results show that when a TF is not used. First the delay is more intensive than a case with TF, second the value of end to send delay is very nearly for booth traffic because the class of service of this application is not the same for UDP. Second when the uses of bandwidth exceed 95% the values of end to end delay are equal. So we conclude that when the traffic became intensive the priority is obsolete

5. CONCLUSION AND FUTURE WORK

In this paper we made an overview of the quality of service for all the layer used for IoT. We also presented the choice of network technology used in simulations.

We presented some QoS features related to the usage of 6lowpan, zigbee and 802.15.4. Our key contribution is the test of usage of TF filed on QoS. The simulations outcomes proved the importance of this field on delay. The presented results open many research perspectives. As a first step we plan to test our idea in 802.154etechnology.

REFERENCES

[1] P.Hoffman L. Masinter, and J.Zawinksi The mailto URL Scheme, IETF Request for Comment 2386 (1998).

[2] Wroclawski J (1997) The Use of RSVP with IETF Integrated Services.RFC 2210 pp: 1-33.

[3] Blake S, Black D, Carlson M, Davies M, Wang Z, et al. (1998) An Architecture for Differentiated Services. RFC 2475 pp: 1-36.

[4] Chen D, Varshney PK (2004) QoS Support in Wireless Sensor Networks:A Survey. International Conference on Wireless Networks .

[5] IEEE 802.15 Working Group fSsor WPAN.

[6] Yigitel MA, DurmazIncel O, Ersoy C (2011) QoS-aware MAC protocols for wireless sensor networks: A survey" Computer Networks 58: 1982-2004.

[7] Li Y, Chen CS, Song Yq, Wang Z (2007) Real-time QoS support in wireless sensor networks: a survey. 7th IFAC IntConf on Fieldbuses & Networks in Industrial & Embedded Systems (FET'07).

[8] IEEE Std 802.15.4 (2006) "Part 15.4: Wireless medium access (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)".Ergen SC, Varaiya P (2006)

[9] PEDAMACS: Power Efficient and Delay Aware Medium Access Protocol for Sensor Networks. IEEE Transactions on Mobile Computing 5: 920-930.

[10] Caccamo M, Zhang LY, Sha L, Buttazzo G (2002) An implicit prioritized access protocol for wireless sensor networks. pp: 39-48.

[11] Watteyne T, Augé-Blum I, Ubéda S (2006) Dual-mode realtime MAC protocol for wireless sensor networks: a validation/simulation approach. InterSense '06 Proceedings of the first international conference on Integrated internet ad hoc and sensor networks.

[12] Saxena N, Roy A, Shin J (2008) Dynamic duty cycle and adaptive contention window based QoS-MAC protocol for wireless multimedia sensor networks. Computer Networks 52: 2532-2542.

[13] Kim H, Min S-G (2009) Priority-based QoS MAC protocol for wireless sensor networks. Parallel & Distributed Processing IEEE International Symposium, Rome, pp: 1-8.

[14] Slama I, Shrestha B, Jouaber B, Zeghlache D (2008) A hybrid MAC with prioritization for wireless sensor networks. 33rd IEEE Conference on Local Computer Networks pp: 274-281.

[15] Rhee I, Warrier A, Aia M, Min J (2008) Z-MAC: a hybrid MAC for wireless sensor Networks. IEEE/ACM Transactions on Networking 16: 511-524.

[16] Yigitel MA, Incel OD, Ersoy C (2010) Diff-MAC: a QoS-aware MAC protocol with differentiated services and hybrid prioritization for wireless multimedia sensor networks.6th ACM workshop on QoS and security for wireless and mobile networks pp: 62-69.

[17] Shelby Z, Bormann C (2009) 6LoWPAN: The Wireless Embedded Internet. A John Wiley and Sons, UK.

[18] Bormann C, Castellani AP, Shelby Z (2012) CoAP: An Application Protocol for Billions of Tiny Nodes.

[19] M. Kirsche and J. Hartwig, "A 6LoWPAN Model for OMNeT++," in Proc. of the 6th OMNeT++ Workshop, co-located with the 6th ICST Conference on Simulation Tools and Techniques