

QoS LowPan for Internet of Things

Neji Kouka^{1*} and Adel thaljaoui²

¹Department of Information Technology, National Engineering School of Tunis University of Tunis El Manar, Tunis, Tunisia

²University of Toulouse-UT2, CNRS-IRIT-IRT, France

*Corresponding author: Neji kouka, Department of Information Technology, National Engineering School of Tunis University of Tunis El Manar, Tunis, Tunisia, Tel: +216 71 874 700; E-mail: koukaneji@yahoo.fr

Received date: May 04, 2016, Accepted date: May 25, 2016, Published date: May 31, 2016

Copyright: © 2016 Kouka N, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

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 effectiveness 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; Sensor networks; Flow label; Traffic class; 6LoWPAN; CSMA/CA; GTS

Introduction

An Internet of Things (IoT) system connects the physical world into Internet via radio frequency identification (RFID) tags, sensors, and mobile devices. IoT is an intelligent collaboration of tiny sensors and devices giving new challenges to the end to end communication of things. 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 scenarios where the network is reasonably loaded (between 40 to 60 %), it is straightforward to apply a priority-based QoS priority in 6LoWPANs. 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.

Related Works

There are two application classes: throughput and delay tolerant elastic traffic and the bandwidth and delay sensitive inelastic (real time) traffic. RFC 2368 [1] definition on internet QoS. QoS refers to an assurance by the Internet to provide a set of measurable services attributes to the end-to-end users in terms of delay, jitter, available bandwidth and packet loss.

QoS support in the Internet can generally be obtained by means of over-provisioning of resources and/or traffic engineering. 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 specific in WSN. The two perspectives of QoS in WSNs described [4], namely applicationspecific QoS and network QoS, represent the two major categories of the existing research for WSN QoS.

QoS at IoT

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

QoS at physical layer

The IEEE 802.15.4 [5] standard defines low-power wireless embedded radio communications at 2.4 GHz, 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 20-50 kb/s data rates depending on the frequency. Channel sharing is achieved using carrier sense multiple access (CSMA), and acknowledgments are provided 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 non beacon-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 super frame that specifies the intrinsic rules to perform such access. The period that specifies the consecutive beacon transmissions is dubbed beacon interval (BI). The super frame structure depicted in Figure 1 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. The CFP was designed to support real-time traffic, being divided in transmission windows dubbed guaranteed time slots (GTSs) that use 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.

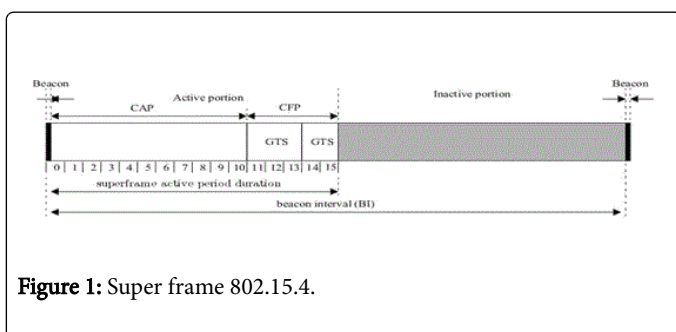


Figure 1: Super frame 802.15.4.

QoS at the stack: ZigBee/802.15.4

We will address the issue of providing quality service to the IEEE 802.15.4 and ZigBee. The MAC can be run in two modes: beaconless mode and beacon-enabled mode. Beaconless mode uses pure CSMA channel access and operates quite like IEEE 802.11 without channel reservations.

Beacon-enabled mode uses a hybrid time division multiple access (TDMA) approach, with the possibility of reserving time-slots for critical data, so QoS can be ameliorated. 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, with 72-116 bytes of payload available after linklayer framing, addressing, and optional security. ZigBee/802.15.4 are an interesting choice for the Internet of Things. The ZigBee protocol stack defines the network and application layers above the physical and link layers standardized by the IEEE 802.15.4. 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 onehop 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.

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 sub layer 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" [6] tried to solve this problem by providing a mechanism for sharing the same "slot" between multiple nodes in the parameters of the traffic flow through them.

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 through the use of routing protocols such SPEED MSPEED and PRAR. 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 realtime applications, generally the Internet of Things. 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.

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 [7,8] respectively. This section below describes the major differences of protocols used to support QoS. The main characteristics of each protocol are described below:

- 1) IEEE 802.15.4 standard [9]: 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 lowrate personal area networks has de facto established as the most suitable, but still not optimal standard for WSN applications.
- 2) PEDAMACS [10]: this TDMA-based protocol that aims to achieve both energy efficiency and delay guarantee (HRT).
- 3) (I-EDF) 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 authors 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.

QoS at network layer

At the network layer, we focus in 6LoWPAN [17] and we look at the impact of the packet compression and fragmentation. In addition, we discuss priority on TF field on QoS.

IPv6 and 6LoWPAN

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] [18]. This field inherits the Type of Service (TOS) in IPv4 header. Hence DiffServ can be transferred seamlessly in IPv4 network to IPv6 network.

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 of the OSI model. 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 or 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).

QoS for Transport layer

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 a new framework for compressing arbitrary next headers, called NHC. 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.

TCP for IoT: QoS problems

Connection setup: TCP is connection oriented and each session begins with a connection setup procedure. 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. Furthermore, the connection setup phase involves data to be processed and transmitted by end-terminals, which in most cases are limited in terms of both energy and communication resources.

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 the destination. In fact, at the source data should be buffered so that it can be retransmitted in case it is lost. At the destination data should be buffered to provide ordered delivery of data to the application. 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. For example, TCP is not able to distinguish between packets dropped because of congestion or packets lost on wireless links.

QoS for Application layer

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 [1], 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 CoAP vs. 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.

Simulation Results

In the simulation we evaluate the QoS in lowpan for the internet of things.

First simulation

In this simulation we evaluate the influence of priority in QoS lowpan for the internet of things. We use in this simulation omnet++, contiki [19].

Architectures of simulations

We chose a network infrastructure as follows in Figure 2.

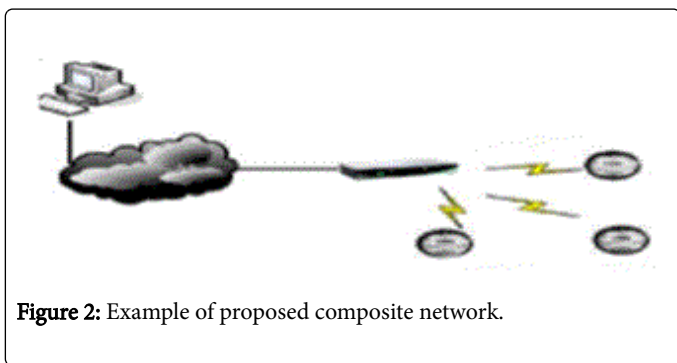


Figure 2: Example of proposed composite network.

Infrastructure, because the routing is not study in this paper we evaluate QoS with a single hop. Table 1 below shows general parameters for simulation.

Parameter	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	Friis Propagation Loss Model
Maximum Bit rate	250 kbps

Table 1: Characteristics of simulation.

The infrastructure network is composed by: N number host of wireless 6LoWPAN/802.15.4 network applications, which are converse with other wired host using 6LoWPAN and Ethernet protocol [20].

*Node how generating UDP streams (as represent a priority traffic). The UDP host with a rate of 16 Kbit/s

*Node how generating Ping streams (as represent no priority traffic) and the PING host with rate 8 Kbit/s.

*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 P/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 vs. increasing of flow. The number of host for each case of simulation is shown below (Table 2).

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

Table 2: Scenarios of simulations.

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.

End to end delay (UDP)

With and without priority (TF)

In Figure 3 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 [21]. 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 Figure 3. 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 value vs. the case of without TF, with a peak of 2.1 ms for the bouth case.

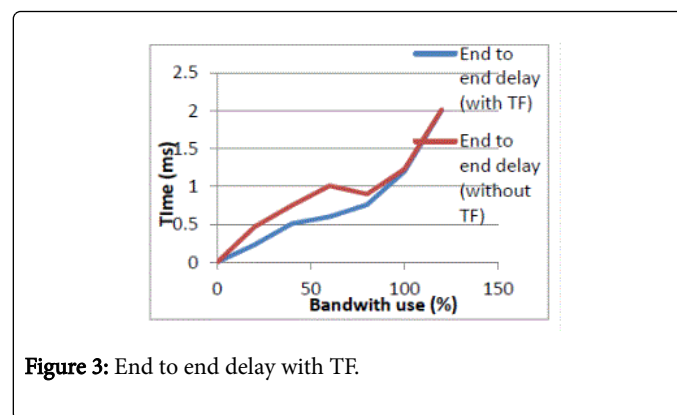


Figure 3: End to end delay with TF.

Each curve contains a peak, which corresponds to the delay during adding of new host. First the QoS for the scenarios with field TF is set when we have a little traffic (Between 0 and 90 %). After that, the TF is obsolete indeed there are same mean end to end delay. So with the result we conclude that TF has an importance when the number of

urgent traffic is less. In fact between 0 and 90% the use of TF in lowpan ameliorate QoS but when they traffic became great the priority has not meaning.

With and without priority (Ping)

Figure 4 demonstrates the mean end to end delay for Ping application with and without use of TF.

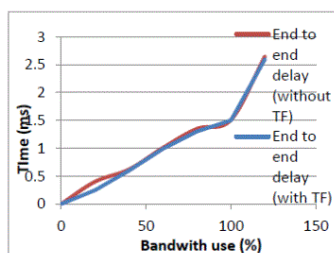


Figure 4: End to end delay with TF.

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 use of bandwidth exceed 95% the value of both traffic are same. So we conclude that when the traffic became intensive the priority is obsolete.

Conclusion and Future Work

In this paper, we have presented studies on the quality of service. We also presented the choice of network technology used in simulations. To perform end to end QoS our goal for future works is how to maintain QoS over heterogeneous networks, and we will focus in QoS for 802.15.4e.

References

- Bormann C, Castellani AP, Shelby Z (2012) CoAP: An Application Protocol for Billions of Tiny Nodes. IEEE Internet Computing 16: 62-67.
- Wroclawski J (1997) The Use of RSVP with IETF Integrated Services. RFC 2210 pp: 1-33.
- Blake S, Black D, Carlson M, Davies M, Wang Z, et al. (1998) An Architecture for Differentiated Services. RFC 2475 pp: 1-36.
- Chen D, Varshney PK (2004) QoS Support in Wireless Sensor Networks: A Survey. International Conference on Wireless Networks 1.
- IEEE 802.15 Working Group for WPAN.
- Yigitel MA, Durmaz Incel O, Ersoy C (2011) QoS-aware MAC protocols for wireless sensor networks: A survey" Computer Networks 58: 1982-2004.
- Li Y, Chen CS, Song Yq, Wang Z (2007) Real-time QoS support in wireless sensor networks: a survey. 7th IFAC Int Conf on Fieldbuses & Networks in Industrial & Embedded Systems (FET'07).
- 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) PEDAMACS: Power Efficient and Delay Aware Medium Access Protocol for Sensor Networks. IEEE Transactions on Mobile Computing 5: 920-930.
- Caccamo M, Zhang LY, Sha L, Buttazzo G (2002) An implicit prioritized access protocol for wireless sensor networks. pp: 39-48.
- 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.
- 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.
- 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.
- Slama I, Shrestha B, Jouaber B, Zeglache D (2008) A hybrid MAC with prioritization for wireless sensor networks. 33rd IEEE Conference on Local Computer Networks pp: 274-281.
- Rhee I, Warriar A, Aia M, Min J (2008) Z-MAC: a hybrid MAC for wireless sensor Networks. IEEE/ACM Transactions on Networking 16: 511-524.
- 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.
- Shelby Z, Bormann C (2009) 6LoWPAN: The Wireless Embedded Internet. A John Wiley and Sons, UK.
- Takai M, Martin J, Bagrodia R (2001) Effects of wireless physical layer modeling in mobile ad hoc networks. In Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing pp: 87-94.
- Kirsche M, Hartwig J (2013) A 6LoWPAN Model for OMNeT++. The 6th International ICST Conference on Simulation Tools and Techniques pp: 330-333.
- Guerreiro A, Jeferson LRS, Rufino J (2013) Improving NS-2 Network Simulator for IEEE 802.15.4 standard operation. 5th Informatics Symposium (INFORUM) pp: 1-12.
- Rajahalme J, Conta A, Carpenter B, Deering S (2007) IPv6 Flow Label Specification. IETF Network Working Group RFC 3697.