Multicast Routing Protocol for LoRa Mesh Networks in Safety Critical Communications

Roberto Di Stefano and Fabrizio Marignetti

Abstract The risk reduction, in case of catastrophic events, is strongly conditioned by the possibility of performing mechanical actuation in extreme conditions and without electric energy. Many devices, which implement security features and fulfill these specifications, are on the market, however the capability to transfer data and information through reliable technologies is also required in order to monitor and coordinate the safety systems. A possible candidate that could provide a communication link, even in the absence of electricity, is LoRa technology, even if it has some problems and limitations mainly due to the topological configuration of the LoRaWAN communication network and the increasing number of devices and users. This paper reports a proposal to improve the reliability of LoRa data transfer in very severe environmental conditions and on large areas. Some accurate simulations conducted on a LoRa network, make it possible to verify the effectiveness of the proposed communication strategy.

1 Introduction

When an extraordinary event occurs in a high-risk environment, it is often necessary to promptly carry out maneuvers aimed at mitigating possible damage and increasing the overall level of safety with regard to people, things, and environment in general. This is especially the case of industrial plants, in which it is necessary to implement fire protection systems, actuate valves to close the flow of dangerous substances, or isolate compartmentalized environments.

Different types of devices able to perform the actuation even in the absence of electricity are present on the market. Their operation is based on the accumulation

R. Di Stefano (✉) · F. Marignetti
DIEI - University of Cassino, Cassino (FR), Italy
e-mail: distefano@unicas.it; marignetti@unicas.it

W. Zamboni, G. Petrone (eds.), *ELECTRIMACS 2019*, Lecture Notes in Electrical Engineering 615, https://doi.org/10.1007/978-3-030-37161-6_55

of mechanical energy in the form of compressed air, or in an elastic form. These actuators are subjected to very strict standards (i.e., ISO 26262, EN 50129, EN ISO 13849-1, IEC 62061, IEC 60601) that regulate the component functional safety on which the system safety as a whole depends. Manufacturers must therefore take all the necessary precautions to minimize the risk of malfunction even when extreme conditions are present, such as high temperatures caused by a fire.

In order to increase the reliability and robustness, during the design and development of the product, it is necessary to implement redundant functions and perform a preventive analysis of the possible causes of failure caused by random or systematic events or errors. As is known, the risk assessment process is essential to define the functional safety requirements. One of the intermediate results of the evaluation process is a list of the functions that allow to mitigate the consequences of failures, each of them characterized by its degree of reliability and the degree of criticality or associated risk [1–3]. The risk assessment process can be completed during the design and testing phase before the final installation. In other cases, it can also be extended during operation period, analyzing and studying the statistics of operation, intervention, maintenance, and failure [4, 5]. This further analysis complements the previous one, constituting in fact a feedback of considerable importance, which allows to detect causes of malfunctioning, which had not been taken into consideration and therefore to carry out, with greater precision, the evaluation of the risk. The result is the possibility of significantly improving the safety integrity level (SIL), increasing the risk reduction factor (RRF), both in a further design phase, or with extraordinary maintenance upgrading the product [6, 7]. It is therefore clear the need to equip these elements with an apparatus capable of detecting in detail the overall state and of carrying out an equally reliable and robust communication [8]. Then the following points worthy of study were identified:

- to study and design a system for detecting the component status;
- to identify an appropriate wireless data transmission and methodology;
- to study and implement a reliable and non-redundant communication protocol that can cover areas of considerable size.

2 LoRa Technology as Candidate in Critical Applications

2.1 LoRa Technology at a Glance

LoRa stands for long-range communication and is a proprietary modulation technique by Semtech, it allows the radio connection across long distance (some kilometers) because of its high sensitivity (10 dB better than GFSK) [9] with low energy consumption. It is derived by the chirp spread spectrum (CCS) [10] with an embedded forward error correction and allows to encode multiple bits (*SF*) per symbol. The transmission frequencies that are usually used are allocated just

below 869 or 928 MHz, other frequencies being used in Asia. A LoRa device requires the setting of many parameters: spreading factor (*SF*), transmission power (*TP*), bandwidth (*BW*), coding rate (*CR*), carrier frequency (*CF*). This makes this technology very flexible as it allows to identify several possible options that have influence on the transmission distance, transmission time, integrity of data, and energy consumption. For this reason, researchers [11–16] have tried to identify general criteria for obtaining the best performances by a suitable combination of parameters setting, also in relation to the environment and the number of devices involved.

2.2 Merits and Defects of LoRaWAN and Others Protocols

LoRaWAN is the link layer protocol designed for LoRa. Its topology is deployed as star of stars, this implies the presence of gateways (nodes) that concentrate the uplink and downlink packets, respectively, from and to end-devices, routing them towards network servers. Since the gateways are connected to a physical network (internet) this implies the functional mix of the two networks: the wireless network is limited in its geographical extension by the possibility of installing gateways; even the functions and reliability of LoRaWAN depend heavily on gateways. In order to better meet the needs of different applications, three different classes of operation have been defined for LoRa devices which are part of a LoRaWAN: Class *A*, which provides for the management of two listening downlink time slots after the transmission of an uplink packet to the gateway. The class *B* which, in addition to slots considered in the operation of class *A*, defines additional listening time slots programmed on the basis of a time synchronization received from the gateway. The class *C* in which the device is continuously listening. Of course, these classes of operation involve a different energy consumption (Class *C* is usually powered by mains) and a different chance that data exchange can be successful. Because each gateway acts as a bridge among the end-devices and the backhaul access, the concentration of the data in a single node has strong implications on the transmission capacity and reliability. There are numerous recent studies that clear up the real limits of LoRaWAN technology in different environmental conditions, also defining analytical models that allow to calculate the real performance of network [16–19]. The probability of packet collision, which could be measured by using packet reception rate(PRR), derives by the difficulty of coordinating uplink transmissions, this dramatically compromises the scalability of network. A further factor that can limit the network size concerns the relation between spreading factor and bit rate is

$$BR = SF \cdot \frac{4}{(4 + CR)\left(\frac{2^{SF}}{BW}\right)}. \tag{1}$$

In fact, in order to limit the time required to transmit the payload, it is necessary to consider lower values of the spreading factor. In Europe, other limitations derive from the compliance with the requirements imposed by the European Telecommunications Standards Institute (ETSI) which requires a duty-cycle for each device not exceeding 1% and a maximum output power of +14 dBm. HART communication protocol born as an industrial automation control protocol on wired infrastructure by means of FSK modulation, superimposed on analog 4–20 mA communication lines. The line has the possibility to transfer both analog and digital information. The protocol has been ported in a mesh wireless 2.4 GHz infrastructure (WirelessHART), of course missing the analog transport, becoming very popular in industrial environment. The network is able to reconfigure itself and has healing capabilities, within certain limits, since it guarantees transmission even in the presence of any faults.

2.3 Other Solution

A mesh-like network is based on a different paradigm, each device also acts as a gateway, propagating the packet received towards the other devices, this allows to overcome the limitations in covering large areas, or characterized by environments that shield the radio waves, such as dull industrial surroundings, or tunnels, or subways. The mesh-type network can be organized, from the logical point of view, into flexible way in order to avoid the concentration of transmissions in a single node, moreover it can dynamically reconfigure itself facing unexpected situations, such as failures, node movements, loss of connection, etc. This property makes transmission of packets much more reliable, reducing the risk of collision, but has the negative effect of increasing latency times, energy consumption, bandwidth limitation. There are three types of multicast routing protocols: the first, called proactive, maintains the routes of group members and those of single nodes that are not part of groups; the second, called reactive, constructs the route when it is required for the transmission of a packet; the third is known as hybrid because it implements a combination of first two. Of course a complete survey of these technologies cannot be reported here, many papers are present in scientific literature, some of them are reported in [20–22]. In [23], Lundell et al. propose an hybrid communication protocol suitable for LoRa networks, however the specifications referred to in these proposals are mainly oriented towards energy saving and rapid dynamic reconfiguration of routing tables.

3 A Different Communication Strategy

3.1 Technical Specifications

A network of sensors for industrial and environmental monitoring is usually not powered by the electricity grid, except in emergency conditions where electricity can be missing. The network topology is substantially static under normal conditions, while it may require a reconfiguration of its paths in case one of the nodes is not available or intentionally excluded. This unavailability can involve even more contiguous nodes, so the ability of the logical network to reconfigure itself must resort to LoRa's technological features in an attempt to establish transmission paths even at considerable distances. The data traffic may not be symmetrical, that is, it may be unbalanced in uplink rather than in downlink, in fact the latter may be related to control remote security systems, while the uplink mainly conveys the communication of the status of devices and environmental conditions. From this point of view, the protocol that seems to be most suitable for this type of network is proactive, such as optimized link state routing protocol (OLSR) that fixes a number of multi-point relays, each of which connects a single pair of nodes. The routing tables are updated only if necessary in order to minimize communication overhead. In the specific case, under normal conditions, the network does not present problems of high traffic density, and does not require special measures to limit the energy required for communications, so it is possible to define a configuration methodology that engages the network especially when the sensors and the actuators are powered regularly and instead have the ability to quickly reconfigure communication paths without performing complex operations when the state of emergency is in place.

3.2 Sensor and Actuators Network

The network topology, which is taken into account in this work, is basically composed of static nodes. They can be connected to sensors and actuators located in an area and installed for different purposes. As an example, a large industrial area may be considered, in which it is necessary to control emergency actuators and monitor some environmental variables, or a metropolitan area where it is necessary to measure the pollution, traffic or, in general, other conditions or variables of interest. The nodes could also be installed in closed environments, such as tunnels, mines, foundries, etc. So it is a network that, from the geometric point of view, is not affected by important changes. The network can be strongly influenced by extraordinary events that can make some nodes inactive, for example, fires, explosions, even simply uncontrolled temperature increases [24]. The proposed communication protocol was designed to allow, as far as technically possible, the transfer of information from one node to another, identifying the best possible route and minimizing the network when a critical situation occurs, exploiting at best the

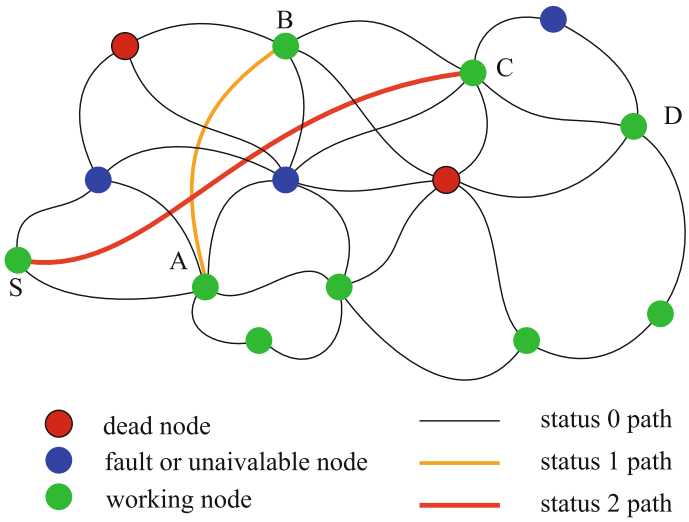

Fig. 1 Possible LoRa network form

characteristics of the LoRa technology. In Fig. 1 a sketch of a possible network is reported. By the way, none of the nodes has backhaul access to internet, even if it could be connected to a local server.

3.3 General Communication Strategy

The proposed communication strategy considers two different operating states, the normal one, in which the nodes are powered by the electric grid or in any case do not have particular energy saving requirements, and the emergency one, during which the network may be affected by losses of connectivity, lack of power, and inactive nodes. When the network operates in normal condition, the communication strategy aims to identify the optimal routes, but it also identifies possible alternatives to be used when alterations of topology occur. In this state, it is preferable that the nodes make periodic reconfiguration attempts to establish a certain number of alternative routes to be stored systematically in hierarchical tables that will be used if the default paths are unavailable. When the network is in emergency state the communication path is chosen among the possible paths stored in the hierarchical tables, it will be discarded if no acknowledge will return back by the destination end-node. In this case another path will be chosen in place. The route switching process will be described in more detail afterwards. This strategy relieves the network from self-commitment and reconfiguring itself when the emergency state is in place, it offers an immediate alternative to communications reducing energy needs just when energy should not be wasted.

4 Communication Handling and Protocol Design

The design of the protocol must consider some aspects that concern both LoRa technology and the limitations imposed by regional regulations. In Europe, there are significant limitations on the duty-cycle, which cannot exceed 1% for each device. This limits the amount of information that can be transmitted for the purpose of determining communication paths and packet size. Considering the node numerosity in the network, the identification of the nodes can be done not using a mac-address formed by 8 bytes, but by an ID formed by a lower number of bytes (i.e., only two) that are set unambiguously during installation. This allows to save on the payload size favoring a higher transmission frequency.

The state of the network can assume different degrees of emergency. The lowest is that in which the status of the nodes is normal operation or in a programmed suspension condition, this state corresponds to the use of the default set of routing tables. The following states correspond to a situation in which one or more nodes cannot guarantee the transfer of information due to unforeseen events. In this case, all nodes use the second set of routing tables. If there is an additional set of routing tables, this will be adopted by all nodes if the second set does not guarantee the transfer of information. The switching mechanism among the statuses must involve all the nodes, in fact it is necessary to maintain consistency between the routing tables adopted by the nodes, because the information stored in the routing tables regards also TX/RX parameters which should have to correspond for all the nodes of the network.

This circumstance is guaranteed only if all nodes use the same tables set. Each node must decide autonomously in what condition to operate on the basis of information received from other nodes or on the basis of information that has not been received.

When the network is in normal operating conditions, it is likely that the maximum distance between a pair of nodes is enough to guarantee efficient communication with a low spreading factor. This allows the frequency of the transmitted packets to be increased, respecting the duty-cycle limit, in order to identify all the possible routes and to create the first routing tables, i.e., those with the highest priority.

When the short communication channels are stable, limited time windows will be set during which a pair of nodes at a greater distance will try to establish a new hop with different TX/RX parameters, for example, with a greater SF. This is achieved by transmitting a packet of Route REQuest (RREQ) to the node with which to connect.

The RREQ defines the TX/RX parameters for test communication between the two nodes and also defines the time parameters within which this transmission will take place, these data are written into payload of the RREQ packet. Therefore, after this exchange of information, there will be a finite time window during which two nodes can establish a test transmission useful to verify the effectiveness of the connection. If the test is positive, the respective routing tables will be updated. The test can fail either because of the weakness of the received signal, or because of the

difficulty in receiving a message without errors. Of course also the receiver time-out produces the same result and therefore the information dumping. Each node then holds two or more sets of routing tables and periodically performs operations that are intended to create and update tables.

The quality of the transmission was performed by considering the values of the RSSI (signal strength indicator received), and the number of errors corrected during transmission of the test messages.

Figure 2 reports the general flowchart of the procedure which is scheduled in the logic of each node.

In this experimental work, the number of routing tables sets is only two, but it could be increased, although it does not seem that more than three sets could further improve the probability that a packet can be successfully transferred. The packet format used for this purpose is shown in Fig. 3.

The packet contains the same fields of standard packets: the identifier of source (S-ID, two bytes), the identifier of destination (D-ID, two bytes), the transmitter identifier (T-ID, two bytes), the receiver identifier (R-ID, two bytes), the type of message (T, one byte), the priority level of the routing table that is attempted to create (Lev, one, byte), the new transmission and reception parameters (TR-Par, six bytes), the temporal characteristics of the window to be used (Window, four bytes).

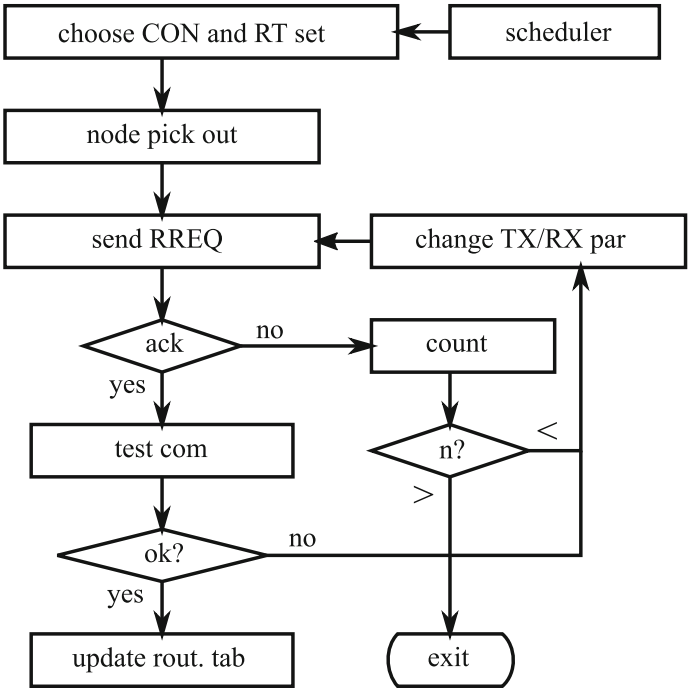

Fig. 2 Diagram of the scheduled procedure to update the routing tables

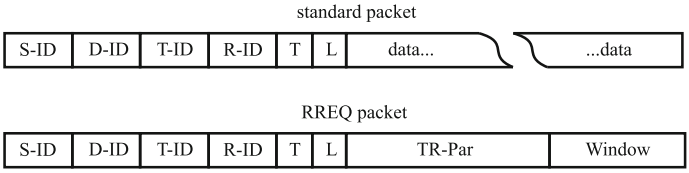

Fig. 3 Route Request (RREQ) packet and acknowledge

Table 1 Routing table

Status	Type T	Dest D-ID	Next relay T-ID	TX/RX parameters TX/RX
0	C	12	8	short
0	D	16	3	short
0	D	16	10	short
1	D	16	16	long
0	S	12	10	short
0	D	12	10	short

The packet has the same format of a standard packet, except for the contents of the identifiers, in fact S-ID and T-ID are the same, as are also D-ID and R-ID. It will be transmitted to a non-contiguous node to ask to establish a new path. The receiving node responds to the request with an acknowledge message sending back the same packet, of course with swapped sending and receive IDs.

4.1 Structure of the Routing Tables

Table 1 shows a possible routing table related to a certain node. The first column shows the status of the node, it is possible to notice how there are two possible paths to the destination 16. The first, relative to the state 0, passes through the relay 10, the second, relative to the state 1, comes directly to the destination node 16 with suitable transmission parameters.

4.2 Management of Communications in States Other than 0

In case a node is unable to communicate with an adjacent one, listed in its RT and marked in 0 state, a verification procedure is activated to assess that such malfunction is due to a permanent failure rather than to a temporary irregularity. At the end of this phase, the node can enter the next state (in this example state 1) and use a different path for routing. State 1 implies different parameters of transmission and reception for some nodes too, so two time windows will be established, even of different sizes, during which the node will switch its TX/RX mode. Naturally,

the information necessary to communicate in these time windows, with the correct transmission and reception parameters, must be transmitted to the adjacent still functioning nodes.

5 Performance Evaluation

The communication strategy and relative protocol have been tested simulating a set of nodes each composed by an embedded LoRa SX1276 module mounted on a nucleo STM32L476RG development board which features an ultra-low-power micro-controller. Some of this modules are also equipped with an IKS01A1 sensor board, which provides numerous environmental data (see Fig. 4). In order to perform a complete and accurate simulation, OMNeT++ has been used. This tool contains a complete set of c++ libraries for simulate many kind of networks topologies also building custom nodes, sensors, and protocols. It allows to evaluate the performance of implemented systems. The most important feature is represented by its modularity, in fact it could be integrated by other frameworks that give facility to simulate off standard networks. The proposed network uses the libraries for LoRa devices (FLoRa) developed at Aalto University School of Science (Finland). The simulation allows to check the statistics of packets lost due to possible collisions, and to measure the dynamics of creation and update of the routing tables. The use of an accurate virtual system is particularly useful for verifying network performance in situations that can hardly be verified experimentally.

Fig. 4 LoRa modules used for experimental tests

6 Conclusions

A methodology for handling a wireless network based on LoRa technology has been designed and implemented. The aim of the proposed technique is to maximize the probability that a given message reach its destination in the same network, even in emergency conditions, i.e., when some nodes in the network are faulty or inefficient.

The communication methodology presents some implementation difficulties that can be overcome. Improvements may be implemented in order to verify the performance and reliability of communications even on networks composed of LoRa nodes with less homogeneous characteristics. Further improvements could include: the management of information security, providing the network with encryption capabilities, and the management of unexpected events such as failures or temporary inefficiency of transmission (for example, due to poor weather conditions).

Acknowledgements The authors acknowledge the financial support of the Regione Lazio thanks to the grant "Progetti di Gruppi di Ricerca finanziati ai sensi della L.R.Lazio13/08."

References

1. Z.E. Bhatti, P.S. Roop, R. Sinha, Unified functional safety assessment of industrial automation systems. IEEE Trans. on Ind. Inf. **13**(1), 17–26 (2017)
2. P. Stirgwolt, Effective management of functional safety for ISO 26262 standard, in *2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS)*, pp. 1–6, Jan 2013
3. T. I. of Electrical and E. E. USA, 2017 National Electrical Safety Code(R) (NESC(R)), in *2017 National Electrical Safety Code(R) (NESC(R))*, pp. 1–405, Aug 2016
4. D. Etz, T. Frühwirth, A. Ismail, W. Kastner, Simplifying functional safety communication in modular, heterogeneous production lines, in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, pp. 1–4, June 2018
5. J.V. Bukowski, Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems. IEEE Trans. Reliab. **50**(3), 321–329 (2001)
6. J.V. Bukowski, A unified model for evaluating the safety integrity level of safety instrumented systems, in *2008 Annual Reliability and Maintainability Symposium*, pp. 137–142, Jan 2008
7. J. Blanquart, P. Baufreton, J. Boulanger, J. Camus, C. Comar, H. Delseny, J. Gassino, E. Ledinot, P. Quéré, B. Ricque, Software safety assessment and probabilities, in *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*, pp. 213–214, June 2016
8. E. Babeshko, V. Kharchenko, K. Leontiiev, E. Ruchkov, V. Sklyar, Reliability assessment of safety critical system considering different communication architectures, in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pp. 17–20, May 2018
9. Semtech, LoRa (TM) modulation basics application note an1200.22. Semtech Corporation - Wireless Sensing and Timing Products Division, Tech. Rep., (2015), https://www.semtech.com/uploads/documents/an1200.22.pdf
10. B. Reynders, S. Pollin, Chirp spread spectrum as a modulation technique for long range communication, in *2016 Symposium on Communications and Vehicular Technologies (SCVT)*, pp. 1–5, Nov 2016

11. M. Bor, U. Roedig, LoRa transmission parameter selection, in *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 27–34, June 2017
12. J. Lim, Y. Han, Spreading factor allocation for massive connectivity in LoRa systems. IEEE Commun. Lett. **22**(4), 800–803 (2018)
13. Z. Qin, J.A. McCann, Resource efficiency in low-power wide-area networks for IOT applications, in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pp. 1–7, Dec 2017
14. F. Cuomo, M. Campo, A. Caponi, G. Bianchi, G. Rossini, P. Pisani, EXPLoRa: Extending the performance of LoRa by suitable spreading factor allocations, in *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1–8, Oct 2017
15. F. Yu, Z. Zhu, Z. Fan, Study on the feasibility of LoRaWAN for smart city applications, in *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 334–340, Oct 2017
16. O. Georgiou, U. Raza, Low power wide area network analysis: Can LoRa scale? IEEE Wireless Commun. Lett. **6**(2), 162–165 (2017)
17. A. Pop, U. Raza, P. Kulkarni, M. Sooriyabandara, Does bidirectional traffic do more harm than good in LoRaWAN based LPWA networks? in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Dec 2017, pp. 1–6.
18. D. Bankov, E. Khorov, A. Lyakhov, Mathematical model of LoRaWAN channel access, in *2017 IEEE 18th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–3, June 2017
19. K.A. Rahman, K.E. Tepe, Towards a cross-layer based MAC for smooth V2V and V2I communications for safety applications in DSRC/WAVE based systems, in *2014 IEEE Intelligent Vehicles Symposium Proceedings*, pp. 969–973, June 2014
20. P. Garnepudi, T. Damarla, J. Gaddipati, D. Veeraiah, Proactive, reactive and hybrid multicast routing protocols for wireless mesh networks, in *2013 IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1–7, Dec 2013
21. K. Pavai, A. Sivagami, D. Sridharan, Study of routing protocols in wireless sensor networks, in *2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies*, pp. 522–525, Dec 2009
22. T.N. Nagabhushan, S.P.S. Prakash, K. Krinkin, Power-saving routing algorithms in wireless mesh networks: a survey, in *2012 11th Conference of Open Innovations Association (FRUCT)*, pp. 107–115, April 2012
23. D. Lundell, A. Hedberg, C. Nyberg, E. Fitzgerald, A routing protocol for LoRa mesh networks, in *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pp. 14–19, June 2018
24. C.A. Boano, M. Cattani, K. Römer, An experimental evaluation of the reliability of LoRa long-range low-power wireless communication. J. Sensors Actuator Netw. (2017). https://doi.org/10.3390/jsan6020007