Proposal of a Hybrid LoRa Mesh / LoRaWAN Network

Nelson C. Almeida
São Paulo State University (Unesp)
Sorocaba, SP, Brazil
nelson.almeida@unesp.br

Rodrigo P. Rolle
São Paulo State University (Unesp)
Sorocaba, SP, Brazil
rodrigo.rolle@unesp.br

Eduardo P. Godoy
São Paulo State University (Unesp)
Sorocaba, SP, Brazil
eduardo.godoy@unesp.br

Paolo Ferrari
University of Brescia (Unibs)
Brescia, Italy
paolo.ferrari@unibs.it

Emiliano Sisinni
University of Brescia (Unibs)
Brescia, Italy
emiliano.sisinni@unibs.it

***Abstract* – There is a recent interest in the deployment of Low Power Wide Area Networks (LPWANs), such as LoRaWAN, to support Internet of Things (IoT) applications. Even though the main advantage of these LPWANs are the long rage communication, the challenge of providing seamless and shadow area coverage still remains. This paper presents a proposal of a hybrid LoRa Mesh/LoRaWAN network to cope with this challenge. In this proposal, a mesh network of LoRa nodes are connected to a Proxy node that works as a mesh coordinator and is also connected to the LoRaWAN network. The advantage of this topology is the improvement of the communication coverage in shadow areas where a regular LoRaWAN node cannot be reachable in cases of obstacles or topography. The development of the LoRa Mesh network as well as the routing mechanism are presented and verified with experimental results. Finally, the integration of the LoRa Mesh with the LoRaWAN networks is discussed and a proposal is presented.**

Keywords – LoRa, Internet of Things, Industry 4.0, AODV protocol.

I. INTRODUCTION

Nowadays, modern Internet of Things (IoT) solutions need to transmit many different data at great distances using wireless communications. There are many different wireless protocols to transmit these data such as Bluetooth, ZigBee, Wi-Fi, cellular 3G/4G or LPWANs. Each one of these protocols has their own characteristics, advantages and disadvantages. For example, Wi-Fi transmits data with higher bandwidth, but the energy consumption is equally higher and usually it is not recommended for battery powered devices. The 3G/4G provides a great coverage for IoT devices but it has higher costs and the energy consumption makes battery life decreases. Finally, the Low Power Wide Area Networks (LPWANs) come to improve this scenario making easy to develop low cost devices that communicate in long range scenarios with lower but compatible bandwidth. In addition, LPWANs also provides higher energy efficiency improving the battery lifetime and network scalability [1].

There are several types of LPWANs such as LoRaWAN, SigFox and NB-IoT, each one also with their own characteristics. The use of LPWANs in IoT applications has risen recently and can be found in various areas such as agriculture, industry, smart cities and homes, smart metering, among others [1, 2]. LoRaWAN is one of the most widely diffused and adopted LPWAN [3], providing a low-cost way to ensure the data reaches long ranges and guaranteeing security using the LoRa physical layer [4].

Considering LoRaWAN devices and traditional applications, there is a great number of studies on the literature [3]. Even with these technologies, in some conditions (star topology) LoRa-based network and LoRaWAN may suffer from coverage issues and shadow areas, where the data cannot be transmitted. For this reason, some studies show a variety of applications that try to extend communication range and cover areas in which a traditional LoRa link cannot achieve [5, 6, 7].

In particular, reference [6] presents the development of an E-node (enhanced node) which can extend the LoRaWAN range by transparently forwarding frames of regular nodes. Other most commons ideas are about developing multi-hop LoRa P2P networks [5], multi-hop for dense building and smart city scenarios [8][9], and LoRa Mesh networks [8] [10]. The reference [5] presents a multi-hop LoRa protocol enabling data to be transmitted in a linear P2P network. In [9] the clear advantage of multi-hop strategy is investigated and demonstrated. A LoRa Mesh network was initially developed in [8]. A mesh network provides communication reliability by means of multiple routes for data transmission. As a result, routing protocols for LoRa Mesh have also been developed in recent papers [11].

In any case the design of a new application layer for the previously introduced solutions may require a huge effort. A more viable solution would be the adoption of the same architecture (and data integration) of the most diffused LPWAN. For instance, LoRaWAN backend infrastructure has been proved to be effective, with full support to security and with multi-app capabilities. In addition, public providers are already operating around the world (e.g. The Things Network, TTN), boosting the data share possibilities of any product that is interfaced with them.

Considering this opportunity, this paper presents a solution to exploit both mesh architecture leveraging a high sensitivity radio based on LoRa and the advantage of the well-established IoT-friendly backend infrastructure of LoRaWAN. The proposed solution is a hybrid LoRa Mesh/LoRaWAN network that preserves both security and application data transparency. The improved coverage will be achieved by means of the LoRa Mesh network. The integration between the LoRa Mesh and the LoRaWAN networks is done by a Proxy node, which keeps for itself the complexity of the LoRaWAN stand, and makes a secure "bridge" between the LoRa Mesh data and the LoRaWAN gateway.

978-1-7281-4892-2/20/$31.00 ©2020 IEEE

II. LoRaWAN Concepts

The LoRaWAN can reach a long-range communication within a range of up to some kilometers with low energy consumption [1]. In this network, LoRa defines the physical layer [4] and LoRaWAN works with the network protocol. LoRaWAN works with the star-of-stars topology in which wireless links provide connectivity between end-devices and gateways and between the gateways and the backend servers, where the network management is handled and the user applications are executed [6]. At this star topology, i.e. one hop topology, each end-device node needs to achieve one or more gateways to deliver your data but, in some situations shadow areas of coverage can appear if obstacles or the topography make this difficult.

The nodes are based on a proprietary physical layer by Semtech where LoRa is an example of Chirp Spread Spectrum (CSS) modulation and the chirp frequency trajectory codes a symbol made of spreading factor (SF) bits. This technique enables that different spreading factors implement virtual channels, due to the quasi-orthogonal nature in different chirps.

The specification of LoRaWAN describes a data link layer, with a medium access strategy that limits the collision in dense environments. In order to optimize a variety of applications, LoRaWAN specification defines three classes, depending on how uplink and downlink are arranged and latency versus battery lifetime. All these classes are bi-directional protocols [6]. Class A offers basic functionalities, lowest power consumption and must be supported by all devices. Each uplink has two short downlinks receive windows, scheduled by the node. Class B, in addition to the Class A, opens extra receive windows at scheduled times. It receives time-synchronized beacon from the gateway, which allows the gateway knows when the node is listening. Class C permits maximum receive slots by extending the second window. Above the datalink, a standardized and decentralized backend takes care of managing the network and handling user applications; the Network Server, the Join Server, and the Application Server are the entities that resides in the backend.

III. Hybrid LoRa Mesh/LoRaWAN Network

In LoRaWAN networks it is known that there are areas where the end-device signals cannot achieve the gateway because of obstacles or topography variations. In these areas, the end-device nodes cannot send data and defines shadow areas in the LoRaWAN coverage. Our solution to this problem is developing a LoRa Mesh network to enable the communication among devices in shadow area, initially not covered by the LoRaWAN, with a Proxy node in the LoRaWAN network, as shown in Fig. 1.

A. The LoRa Mesh

The hybrid LoRa Mesh/LoRaWAN maintains the compatibility with the legacy LoRaWAN network. The LoRa Mesh network has a coordinator, which is called Proxy node. The Proxy node is compatible with LoRaWAN and interconnects the data or devices from LoRa Mesh network with the LoRaWAN network. The Proxy node is also the coordinator of the LoRa Mesh: it is responsible for the management of mesh routes and receive/forward mesh packets to the LoRaWAN gateways.

The proposal of the hybrid LoRa Mesh/LoRaWAN network presented in Fig.1 is to improve the network coverage in shadow areas, although it would be possible to extend the LoRaWAN coverage to areas where LoRaWAN nodes cannot send packets to your nearest gateway. As a result, the proposed LoRa Mesh network does not necessarily need to support a great number of hops or nodes. The LoRa Mesh in this proposal was developed in a way each mesh network can have up to 6 devices and the communication between the LoRa Mesh end-node and the Proxy node can have up to 3 hops. According to Fig.1, the coverage in LoRaWAN shadowed areas (marked in gray) would be improved by positioning LoRa Mesh nodes within this area. In addition, it is also clear that the overall coverage of the hybrid Lora Mesh/LoRaWAN network (blue and green circles) might could also be improved when compared with only the LoRaWAN itself (blue circles).

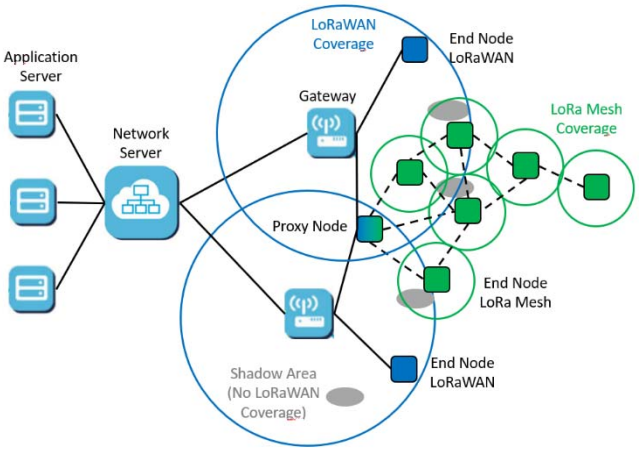

Fig. 1: Architecture of the Hybrid LoRa Mesh / LoRaWAN Network.

The Proxy node implements a simplified Ad-hoc On-Demand Distance Vector (AODV) routing protocol in order to define the routes for communication between each LoRa Mesh end-node with the Proxy node. The AODV protocol meets the proposal needs for routing and was chosen due its simplicity. This simplified AODV utilizes some features of original AODV protocol [12] and a hybrid routing technique [13]. These AODV features include RREQ and RREP signalizing, route cost, route life time and the route table is updated on demand.

Each node in the LoRa Mesh has a unique identifier. Therefore, the Proxy node can identify from which LoRa node the data/message is coming from. The Proxy node associates each message to a virtual LoRaWAN node and retransmits it to the LoRaWAN gateway (see section B). The next LoRaWAN communication steps (gateway, network server, application server) follows the traditional path.

B. Integration of LoRa Mesh/LoRaWAN

In order to integrate the LoRa Mesh inside LoRaWAN infrastructure, two main strategies can be used:

- Data Aggregator: the coordinator of the LoRa Mesh is also a normal LoRaWAN node. All the data collected in the mesh network are packet together and are sent as a single message to the LoRaWAN backend.
- Proxy: the coordinator of the LoRaMesh maps every mesh node to a “virtual” LoRaWAN node. As a result, in the

LoRaWAN backend every mesh node is uniquely identifiable.

The very small payload of LoRaWAN messages (especially for SF > 9) would force the Data Aggregator solution to use mini-payload in the mesh network or, alternatively, very few nodes in the mesh network. Clearly, the applicability of this architecture will be reduced to a limited number of scenarios.

For this reason, this work proposes to use an integration based on Proxy in accordance with [6], which enables the virtualization of motes operating with the same radio interface. From the operation point of view, the Proxy must behave like several LoRaWAN nodes at the same time, but the security of the LoRaWAN network must not be violated.

In order to obtain the desired security, the proposed proxy mechanism implements the following features in each Mesh node:

- Each Mesh node is loaded with two unique numbers: the DevEUI and the AppKey;
- Each Mesh node is programmed with a "encryption function" that can be used to cypher the answer to specific requests of the Proxy node (challenge-response mechanism).

The Proxy implements all the LoRaWAN PHY management, while the MAC parts of the message is obtained with the contribution of the Mesh node that knows the security keys.

For the LoRaWAN joint procedures, the Mesh node is asked by the Proxy to use his encryption function (with its very own keys) on the payload of both LoRaWAN joint request and joint response. If the joint response is positive, the result of the deciphering of the joint response is the NwkKey that is stored inside the Proxy.

After the joint, all the following data exchange with the LoRaWAN infrastructure obeys to following rules:

- Uplink: the Mesh node creates the MAC payload and cypher it using the encryption function and its unique keys. After encryption, data are sent using the LoRa Mesh to the Proxy. The Proxy completes the PHY packet and signs it with the NwkKey. Of that Mesh node. In details, the proxy uses the NwkKey for creating the MIC of the LoRaWAN messages.
- Downlink: the proxy extracts the MAC payload form the received LoRaWAN message. Then, it forwards the information to the Mesh nodes using the LoRa Mesh. The mesh node uses its encryption function to decipher the received data.
- In case a Mesh network is not participating to the LoRa Mesh anymore, the Proxy deletes the corresponding NwkKey.
- A new joint request for a Mesh node will overwrite the previously stored NwkKey.

The proposed implementation of the Proxy function allows to maintain the confidentiality of both Mesh node and LoRaWAN data. In case an attacker compromises the proxy, the security of the LoRaWAN is not jeopardized, since the Proxy only knows the network session key of the Mesh nodes.

It is worth mentioning that the Regulations impose constrains on the use of the radio band and limits the transmission time by means of the Duty Cycle (DC) concept. The DC is defined as the ratio between the duration of the transmission and the time distance between two consecutive transmissions. Each LoRa node should obey to Regional Regulation, and this is true also for Proxy node. In particular, the Proxy should respect the limits counting both all the message sent in the LoRa Mesh, and all the message sent in the LoRaWAN network. With the proposed Proxy architecture, the impact of stringent DC limit can be mitigated adopting a pool of Proxies, which share between them the data exchange between LoRa Mesh and LoRaWAN (this topic will be discussed in future works).

The importance of a dynamic scenario forces the use of reactive routing protocols, like AODV and DSR discussed in [14]. In particular, in this paper the use of AODV for implementing LoRa Mesh is preferred because it is already used by traditional wireless sensor networks and has better performance with respect to DSR [14].

Concluding, after the demonstration of the feasibility of the Proxy node, the next step is the characterization of the performance of the mesh subnetwork. In the following the discussion about the use of AODV for implementing LoRa Mesh is presented.

IV. LoRa Mesh Development

The hardware of the LoRa Mesh devices (end-nodes and Proxy node) uses the low cost Heltec ESP32 LoRa modules, which contains an ESP32 SoC and a Semtech LoRa radio SX1276 as shown in Fig. 2. Some characteristics of this module are [15]: MCU 240MHz Tensilica LX6 dual core, Memory 520KB RAM, Wi-Fi and BLE connectivity, LoRa bands EU 863-870, AU-US 902-928, 0.96 inch 128*64 OLED display and 8MB (64M-bits) SPI Flash.

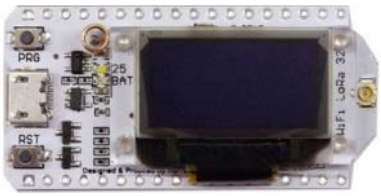

Fig. 2: Heltec ESP32 LoRa module

The software of the LoRa Mesh devices was developed on Arduino IDE and was based on the Heltec LoRa libraries available for the module and on AODV libraries. The main part of the software is the routing mechanism for the mesh network, as all communication are from one device to another (P2P). The mesh protocol implements a simplified AODV in order to discover the nodes and implements the route through the network. This simplified AODV works as follows:

A. End-nodes wait for Route Request packet (RREQ);
B. Proxy node sends the RREQ in broadcast for any near node;
C. When one node receives a RREQ package, it updates the route table and reply a Route Reply Packet (RREP) addressed to the sender and resends a new RREQ to other nodes.
D. If a RREQ was not answered, the node has a route and can now transmit your data at a preconfigured interval;

E. If a node receives RREQ, it updates your route table and returns a RREP that will carry out the route back to the Proxy node;

F. When the Proxy node receives a RREP packet, it will update your route table, control a route lifetime and wait for the data of the nodes.

The time for the first valid route varies with the spreading factor configured. At the present case with a configuration of SF9, the time the first node response with a RREP is 400ms. However, as the Lora Mesh end nodes wait 2s for another neighborhood node responding with other RREP, indicating that there are more nodes to communicate, the route creation time will depend on the number of nodes and hops on the route created. After the route creation, each node can start the transmission of its packets.

The route is updated (new creation) according to two parameters: a specified number of received packets in the Proxy node or a reception timeout (time without any reception). This mechanism updates the routes and maintains the mesh network communicating even if a node disconnects of or is added to the network providing a continuous functioning of the mesh.

In order to exemplify the routing mechanism of LoRa Mesh protocol, consider a case with four LoRa Mesh nodes with the following unique identifications: Proxy node - 0x65, Node 1 - 0xAA, Node 2 - 0xBE, Node 3 - 0xD4. The routing mechanism procedure is shown in Fig. 3 and will be repeated at each configured interval (LoRa Mesh route creation interval), in order to deal with route modifications and add or removal of devices in LoRa mesh network.

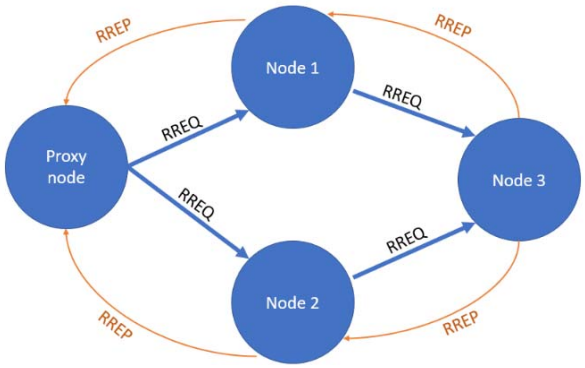

Fig. 3: LoRa Mesh Route Creation: RREQ and RREP process

According to the mesh protocol, the closest route is chosen by the sum of RSSI of the received packets. The lower is the sum the closest is the route between the desired end-node and the Proxy node. The resulting routing schema for the example is shown in Fig. 4.

At the Proxy node, there are table of neighbor nodes and routes to make simple send data or command to any node, directly when it is near or over a route. Each LoRa Mesh node can communicate with each other making this mesh network addressable for receiving data from any node at the Proxy node. Also, the same is true when one LoRa Mesh node needs to receive a downlink from the application at the LoRaWAN server. This simplified AODV protocol was deployed to the LoRa Mesh nodes and the required functionalities were tested.

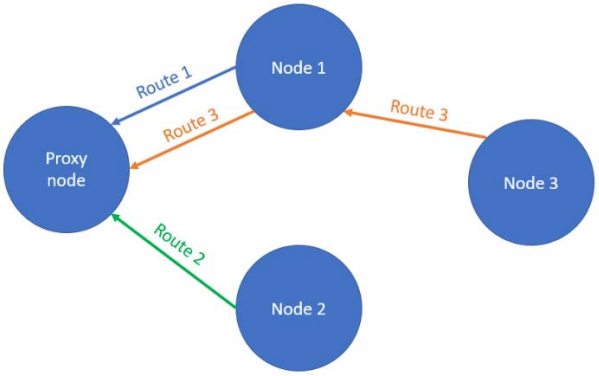

Fig. 4: LoRa Mesh Route Creation: Routes between the nodes.

V. Results and Discussion

In order to verify the operation of the developed LoRa Mesh network, experimental results as a proof-of-concept were done. For this test, the LoRa Mesh nodes (Proxy node and end-nodes) were configured to replicate the received LoRa messages via serial port for debugging purposes. Each LoRa Mesh end-node sends the data of Temperature and Humidity from a DHT11 sensor at an interval of 30 s, which is configurable.

The LoRa Mesh nodes were positioned nearby the Unesp campus in accordance to the Fig. 5. The distances between each node and the Proxy node were: Node AA – 100 m, Node BE – 120 m and Node D2 – 100 m. The transmission power of the devices was programmatically decreased in order to facilitate the tests (decreasing coverage distance between nodes). These distances were enough to guarantee that there was not communication between Node D2 and Proxy node but also considering some obstacles like the buildings and trees of the campus.

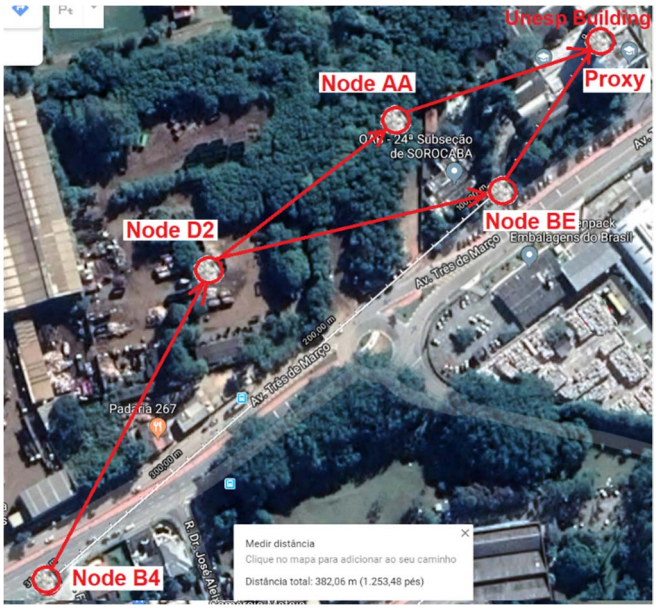

Fig. 5: LoRa Mesh Network Test (arrows show the data transmitted)

The scenario in the test consisted of five nodes in the LoRa Mesh network with up to 3 hops for communication

within the Proxy node. During the route creation, the Proxy node asks the route via RREQ and receives the RREP answers form each node for the route creation. Fig. 6 shows at the serial debug port the data packets received from the LoRa Mesh nodes at the Proxy node.

During the test, the Node BE is sending data directly to the Proxy node and the furthest Node D2 sending data to the Proxy via Node BE. Each data packet has an identifier (id) that indicates the sender of the received message and a route parameter (route) that shows the forwarding node. A route parameter of 0x65 (Proxy Node) indicates a direct transmission (no hop). A different value indicates the node (ex: 0xBE) that forwarded the message from one sender (Node D2 - 0xD2) to the Proxy node.

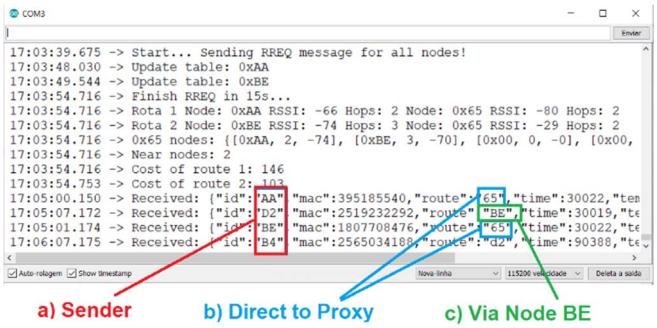

Fig. 6: Debug port at Proxy node: a) Identifier (id) of the sender node, b) Route parameter of the forwarding node (0x65 value means a direct transmission) and c) Proxy node receives data via Node BE

Fig. 7 shows the debug port of Node BE, in which the possible routes (route table) can be shown. There are two routes: Route 1 for a direct connection between Node BE and Proxy node. And Route 2 for a connection between Node AA and Proxy node through Node BE.

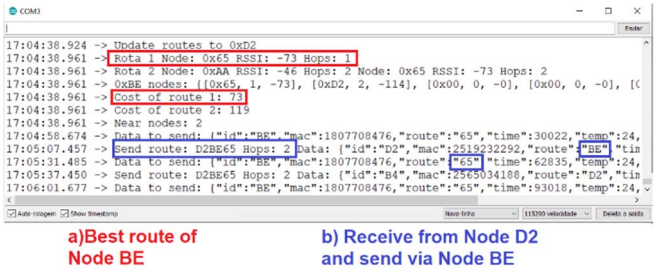

Fig. 7: Route table and the data through Node BE: a) Route to Proxy node (65) and b) Route "D2BE65" passing through Node BE.

Fig. 8 shows the debug port of Node D2, in which the possible routes (route table) can be shown. There are two routes: Route 1 for a connection between Node D2 and Proxy node through Node BE. And Route 2 for a connection between Node D2 and Proxy node through Node AA. These two routes are presented in Table I.

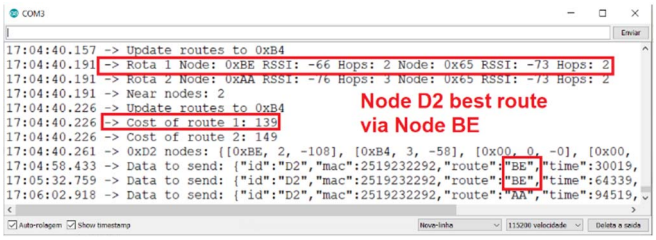

Fig. 8: Debug port at Node D2: Route table and definition of route.

Each route table is formed with the data received from the LoRa Mesh links and are used to determine the best route for communication. The sum of the RSSI value of each hop in the route indicates the route cost in the mesh. The smallest cost determines the best route for communication. As a result, at the scenario of the test (Fig. 5), the best route for communication from Node D2 to Proxy node is through Node BE as shown in Fig. 8.

TABLE I. ROUTE TABLE OF NODE 3 (0XB4).

	Route table	Cost
Route 1	0xAA RSSI: -66 Hops: 2 Node: 0x65 RSSI: -80 Hops: 2	146
Route 2	0xBE RSSI: -74 Hops: 2 Node: 0x65 RSSI: -29 Hops: 2	103

This route table of Node D2 indicates that the best path is send data throw Node BE with RSSI -74 and this is informed by Node BE via RREQ where the Node B4 can update your route table, this indicates too that the Node BE has a LoRa link with the Proxy node (65) with RSSI -29, this route has a cost of 103 with 2 hops to arrive the Proxy node.

In order to validate the mesh communication and verify the route update mechanism, an experiment was done. In this experiment one end-node was stopped. The disconnection of the Node BE caused a broken route to D2 and B4 nodes (Fig. 5). As a result, a route reconfiguration on the Proxy node is done in order to reestablish the communication among the nodes.

Fig. 9 presents the debug of the reconfiguration notation and the new route found through the Node D2 sending information via Node AA. The route creation debug view can be seen in Fig. 10.

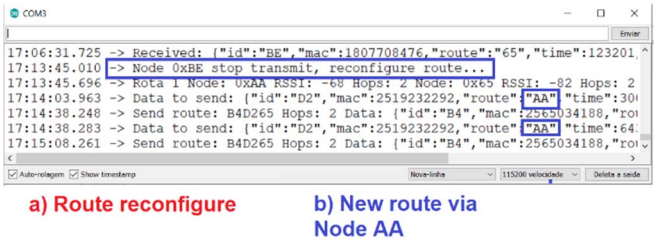

Fig. 9: Route reconfiguration to Node AA.

```
17:03:39.675 -> Start... Sending RREQ message for all nodes!
17:03:48.030 -> Update table: 0xAA
17:03:49.544 -> Update table: 0xBE
17:03:54.716 -> Finish RREQ in 15s...
17:03:54.716 -> Rota 1 Node: 0xAA RSSI: -66 Hops: 2 Node: 0x65
```

Fig. 10: Details of the route creation debugging

In order to analyze the communication performance of the LoRa Mesh network, the route creation and the node transmission times were calculated using the time stamp of the debug log. The time stamp for nodes AA, BE and D2 transmitting to Proxy can be shown in Fig. 11.

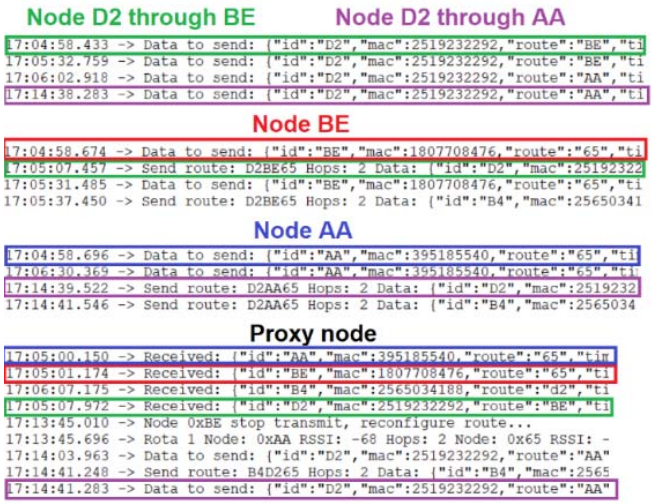

Fig. 11: Time stamp of LoRa Mesh end-nodes transmissions

The calculated route creation time and transmission times from the end-nodes to the Proxy node in the LoRa Mesh were compiled in the Table II. For the experiment done (Fig. 5), the average time for route creation was 15 s. The end-nodes transmission times are different they are related to the communication route.

TABLE II. TIME STAMP FOR THE LORA MESH NETWORK.

Event	Average time(s)
Route creation	15
Transmission from Node AA to Proxy node (1 hop)	1.5
Transmission from Node BE to Proxy node (1 hope)	2.5
Transmission from Node D2 to Proxy through Node AA (2 hops)	3.0
Transmission from Node D2 to Proxy through Node BE (2 hops)	4.4
Transmission from Node B4 to Proxy through Nodes D2 and AA (3 hops)	6.2
Transmission from Node D2 to Proxy through Nodes D2 and BE (3 hops)	7.5

The analysis of the route tables and the verification of communication between the LoRa Mesh nodes and the Proxy node in the test prove the operation of the LoRa Mesh developed. Other tests were done successfully for testing new route creation and communication using different routes. With the development of the LoRa Mesh part of the Hybrid LoRa Mesh/LoRaWAN network, the next step is to integrate this network with the LoRaWAN.

VI. CONCLUSION

This work presented a proposal of a hybrid LoRa Mesh/LoRaWAN network to improve coverage and cope with shadow areas. Operational details of the proposal and architecture components were explained. The LoRa Mesh network uses a simplified AODV protocol. The Proxy node is the coordinator of the LoRa Mesh and the responsible to retransmit messages from the mesh devices to the legacy LoRaWAN. Experimental tests with the deployment of a LoRa Mesh network validated its operation. A discussion about the LoRa Mesh integration with the LoRaWAN is presented highlighting the proposals and challenges. The final version will focus on the timing analysis (latency and time distribution) of LoRa Mesh creation and communication.

REFERENCES

[1] Mekki, K., Bajic, E., Chaxel, F. And Meyer, F. “A comparative study of LPWAN technologies for large-scale IoT deployment”, ICT Express, vol. 5, no. 1, pp. 1-7, 2019.

[2] Luvisotto, M., Tramarin, F., Vangelista, L. And Vitturi, S. "On the use of LoRaWAN for indoor industrial IoT applications, Wireless Communications and Mobile Computing", vol. 2018, ArticleID 3982646, 2018.

[3] Pasetti, M., Rinaldi, S., Sisinni, E., Ferrari, P., Ragaini, E., Longo, M., Zaninelli, D. "On the Use of Synchronized LoRaWAN for the Coordination of Distributed Energy Resources in Smart Grids", 2019 AEIT International Annual Conference (AEIT), Florence, Italy, pp. 1-6., 2019.

[4] SEMTECH (2015). LoRa Modulation Basics, Application Note AN1200.22, 26p.

[5] Abardo, A., Fort, A., Landi, E., Mugnaini, M., Panzardi, E., Pozzebon, A., "Black Powder Flow Monitoring in Pipelines by Means of Multi-Hop LoRa Networks," 2019 II Workshop on Metrology for Industry 4.0 and IoT (MetroInd4.0&IoT), Naples, Italy, pp. 312-316, 2019.

[6] Sisinni, E., Ferrari, P., Carvalho, D. F., Rinaldi, S., Flammini, A., Depari, A. "A LoRaWAN range extender for Industrial IoT," IEEE Transactions on Industrial Informatics, 16 (8), art. no. 8933469, pp. 5607-5616, 2020.

[7] Lee, H.; Ke, K., "Monitoring of Large-Area IoT Sensors Using a LoRa Wireless Mesh Network System: Design and Evaluation," IEEE Transactions on Instrumentation and Measurement, vol. 67, no. 9, pp. 2177-2187, Sept. 2018.

[8] Liao, C.-H., Zhu, G., Kuwabara, D., Suzuki, M., Morikawa H. “Multi-Hop LoRa Networks Enabled by Concurrent Transmission,” IEEE Access, vol. 5, pp.21430–46, 2017.

[9] Aslam, M.S., Khan, A., Atif, A., Hassan, S.A., Mahmood, A., Qureshi, H.K., Gidlund, M., "Exploring Multi-Hop LoRa for Green Smart Cities," IEEE Network, vol. 34, no. 2, pp. 225-231, March/April, 2020.

[10] Cilfone A.; Davoli L.; Belli L.; Ferrari G., “Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies”, Future Internet, vol. 11, 2019.

[11] Lundell, D.; Hedberg, A.; Nyberg, C.; Fitzgerald, E., "A Routing Protocol for LoRa Mesh Networks," IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Chania, pp. 14-19, 2018.

[12] Zhang, Y. Luo, J. Hu, H., “Wireless Mesh Networking Architectures, Protocols and Standards”. Auerbash Publications, New York, 2007.

[13] Singh, K., Behal, S., “A Review on Routing Protocols in Wireless Mesh Networks” Available: International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 2, no. 2, 2013.

[14] Varghese S.G., Kurian C.P., George V.I., John A., Nayak V., Upadhyay A., “Comparative study of ZigBee topologies for IoT-based lighting automation”, IET Wireless Sensor Systems, vol. 9, no. 4, pp. 201-207, 2019.

[15] HELTEC AUTOMATION. ESP32 Lora module specifications. Available: https://heltec.org/project/wifi-LoRa-32/. [Accessed Feb-2020].