On the Dynamics of the RPL Protocol in AMI Networks under Jamming Attacks

Joao R. R Renofio*, Marcelo E. Pellenz*, Edgard Jamhour*, Altair Santin*, Manoel C. Penna* and Richard D. Souza†
*PPGIa, Pontifical Catholic University of Parana – Parana, Curitiba, Brazil
†CPGEI, Federal University of Technology – Parana, Curitiba, Brazil
{jrrenofio,marcelo,jamhour,santin,penna}@ppgia.pucpr.br, richard@utfpr.edu.br

***Abstract*—The Advanced Metering Infrastructure (AMI) is a key component of the Smart Grid architecture. The Neighborhood Area Network (NAN) is the portion of the AMI that enables two-way communication between electric, gas and water meters and City Utilities. Many companies are currently deploying wireless NAN architectures based on the IEEE 802.15.4g technology while the Routing Protocol for Low-Power and Lossy Networks (RPL) has been considered as the mesh routing protocol. In this paper, we investigate the dynamics of RPL for routing path maintenance in the presence of jamming attacks. A precise interference model is implemented and tested under a fully compliant RPL draft implementation. The quality of the survivors routing paths in terms of ETX metric is investigated for different density of gateways. The results provide insights for an efficient NAN design in order to minimize the impacts of jamming attacks in the RPL performance.**

***Index Terms*—RPL, NAN, AMI, Interference, Resilience, Smart Grid**

I. Introduction

The Smart Grid [1] is a new concept for the legacy power grid. It basically consists of a network that integrates the use of communication technology with the electric power infrastructure. This architecture can significantly improve the robustness and efficiency of the generation, transmission and distribution of the electrical systems. The Advanced Metering Infrastructure (AMI) is a fundamental component of the Smart Grid and it allows two-way communication between electric, gas and water meters and City Utilities [2]. The set of smart meters which are connected to a specific gateway, in a particular geographical region, defines the Neighborhood Area Network (NAN). The NAN nodes should be able to send and receive data from the gateway [3].

The NAN plays an important role in the deployment of the Smart Grid. Many communication strategies could be applied in this network. However, wireless technologies have been widely used due to the low cost and ease of deployment. Among all available wireless standards, those enabling mesh architectures allow smart meters to dynamically establish ad-hoc communication with neighbors and find alternative paths to communicate with the gateways, increasing the network connectivity and resilience.

The Routing Protocol for Low-Power and Lossy Networks (RPL) [4] is a recent standard that proposes an IPv6 compatible routing protocol that can be applied in the wireless NAN. Recently, many studies have considered the applicability of the RPL for AMI networks [5] [6] [7]. The RPL builds a routing topology formed by one or more DODAGs (Destination Oriented Acyclic Graphs). Each DODAG is rooted in a single destination, usually representing a node that performs a connection to a backhaul. A DODAG differs from a traditional tree because it permits a node to have more than one parent in the direction of the root. According to the standard definition, RPL uses a slow proactive process to construct and maintain a routing topology, and a reactive and dynamic process to resolve route inconsistencies. RPL uses the *Trickle algorithm* [8] which determines that in steady state protocol operation, control messages are sent at a slow rate, but can be quickly increased to solve inconsistencies.

There are few studies [9] [10] [11] about the jamming effects on the RPL behavior. In multihop networks besides the intraflow and interflow interference generated by the concurrent network traffic, there is the possibility of jamming attacks generated by malicious nodes. The time it takes for the protocol to react to the jamming attack, the number of affected nodes and the quality of the reconfigured routing paths are important questions which help to optimize the RPL operation and trickle algorithms. In this paper, we investigate how RPL reacts against intentional jamming attacks. We consider AMI networks based on IEEE802.15.4g technology [12]. AMI networks present strong performance requirements in terms of two-way communication [13].

Specifically, we investigate how the NAN resilience is affected by the jamming by evaluating the number of isolated network nodes and the link metric of the RPL routing paths after the network re-organization. Our analysis considers a fully compliant RPL draft implementation with Trickle algorithm, a realistic topological model for the AMI network and a precise jamming model. The results provide important insights about the RPL dynamics under different interferer power levels and a number of gateways in the NAN topology.

The remainder of this paper is organized as follows. Section II presents the related work. The employed topological model for the NAN is presented in Section III. A brief review of the RPL protocol is presented in Section IV. Section V describes the mathematical formulation for the wireless channel model and the numerical results are presented in Section VI. Finally, this paper is concluded in Section VII.

II. Related work

The impact of jamming attacks on the performance of Wireless Sensor Networks (WSNs) was investigated in [9] for different attack strategies in a network employing an ad-hoc routing protocol. A cluster-based scenario using the LEACH protocol was also investigated. Their studies were focused only on the data traffic performance metrics and it is specific for the employed routing protocol. In [10] the authors incorporate an interference-based routing metric into the RPL protocol for application in multigateway AMI networks. The metric quantifies the self-network interference generated from both intraflow and interflow traffic. The presence of intentional jamming attacks is not considered and the dynamics of the RPL protocol is not investigated.

In [11] the authors investigate the problem of modeling and detecting jamming attacks in time-critical wireless networks used for cyber-physical systems like the Smart Grid. The paper focuses on the design of a jamming detection system. However, the detailed analysis of the AMI architecture requires a more realistic topological model for the NAN, instead of the classical random and grid approaches [14] [15]. A recent study developed in [16] proposes an interesting strategy for NAN topology generation based on a real map that creates topologies from buildings of an urban geographical area. Inspired by the model proposed in [16] and aiming not to use specific geographical map information, we present in Section III a simple strategy to generate NAN topologies for the study of the RPL protocol.

III. Topological Model for NAN

Typically, in real NAN deployments, the smart meters are positioned on the border of the blocks and near the street. Therefore, based on the study presented in [16], we define a new topology generation strategy in which the nodes are randomly placed in restricted regions, based on practical deployment observations. Consider a street divided in blocks with dimensions (l, l) and a maximum distance c from the border of the block. This defines a peripheral region of a block, where we assume that the NAN elements (smart meters, repeaters and gateways) can be deployed. In order to create a more embracing topology, we can define a street width r and create topologies with more blocks. An example of this structure considering four street blocks is presented in Figure 1. Using the structure that defines the possible regions where nodes can be positioned, the NAN topology elements are drawn using a uniform random distribution. Figure 2 illustrates an example of the topology generated using this model. The results presented in Section VI assume this model to generate the NAN topologies.

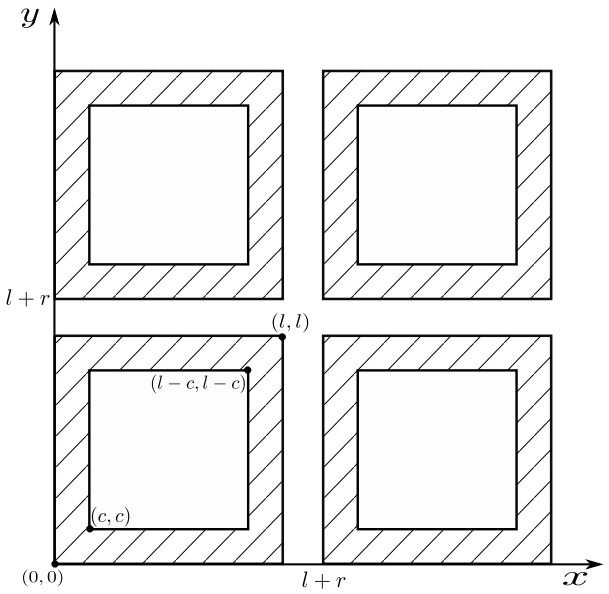

Figure 1. NAN deployment area.

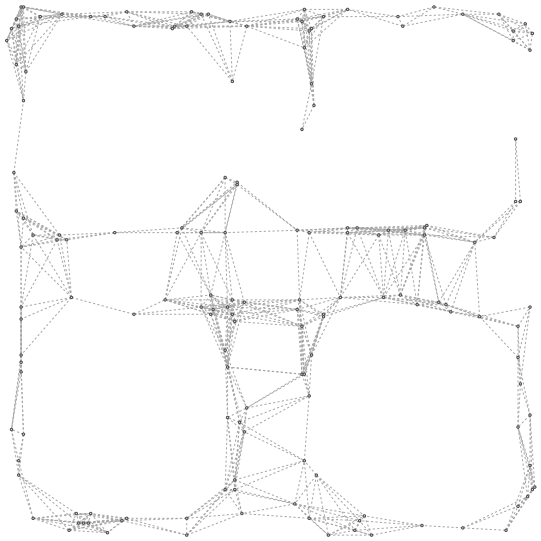

Figure 2. Example of the proposed NAN topology.

IV. RPL Protocol

The AMI is considered a Low-power and Lossy Network (LLN) which is typically made up of embedded devices with limited processing, memory and power resources [6]. In a typical AMI network architecture, the smart meters are connected through IP network to a gateway. The gateways that interconnect an LLN to the backhaul are called LLN border routers (LBRs). There may be several LBRs connecting an LLN to a backhaul or backbone link.

The routing paths in the mesh between a network node and the nearest LBR may be composed of several ways. Typically, in current AMI deployments, the metering applications require all smart meters to communicate with a server, deployed in the utility company data center. This server generates data traffic to configure smart data reading or initiate queries and use unicast and multicast to efficiently communicate with a single device or groups of devices, respectively. Each smart meter generates data traffic according to a schedule, in response to

on-demand queries, or in response to some local event. The RPL has been considered as a possible routing protocol for the NAN in the AMI architecture [6].

The RPL [4] is an IPv6 routing protocol for LLNs that specifies how to build a Destination Oriented Directed Acyclic Graph (DODAG). The RPL builds a Directed Acyclic Graph (DAG) routing structure rooted at an LBR, which ensures loop-free routing and provides support for alternative routes, as well as a wide range of routing metrics and policies. The RPL routing protocol specifies a new set of ICMPv6 control messages to exchange graph related information. These messages are called DIS (DODAG Information Solicitation), DIO (DODAG Information Object) and DAO (DODAG Destination Advertisement Object). The DIO is the main source of routing control information and may store information like the current Rank of a node, the current RPL Instance, the IPv6 address of the root, etc. DAO enables the support of down traffic and it is used to propagate destination information upwards along the DODAG. DIS makes it possible for a node to request DIO messages from a reachable neighbor. An objective function operates on a combination of metrics and constraints to compute the network path in order to create a DODAG.

The RPL provides routing functionality for mesh networks that can scale up to thousands energy-constrained devices and includes energy-saving mechanisms and energy aware metrics. The protocol tries to avoid routing loops by computing a node's position relative to other nodes with respect to the DODAG root. This relative position in the DODAG is called Rank and it increases for nodes farthest from the root and decreases for nodes closest to the root. Many routing protocols broadcast control packets at a fixed time interval which causes energy to be wasted when the network is in a stable condition. Thus, RPL adapts the sending rate of DIO messages by extending the Trickle algorithm. Trickle was designed to be density-aware and perform well in networks characterized by a wide range of node densities. The combination of DIO packet suppression and adaptive timers for sending updates allows Trickle to perform well in both sparse and dense environments.

In most scenarios, the electric meters are powered by the grid they are monitoring and they are not energy-constrained. Instead, electric meters have hardware and communication capacity constraints that are primarily determined by the equipment cost and secondarily by the power consumption. For this reason, the use of RPL storing or non-storing mode should be deployment specific. When meters are memory constrained and cannot adequately store the routing tables necessary to support hop-by-hop routing, RPL non-storing mode should be preferred. On the other hand, when nodes are capable of storing such routing tables, the use of storing mode may lead to reduced overhead and route repair latency.

LLN deployments may utilize link technologies that may exhibit significant packet loss and thus require routing metrics that take packet loss into account. RPL supports a flexible set of metrics and constraints [17].

A. ETX Theoretical Model

In the case of AMI deployments using wireless technologies, the path quality over the link can be characterized by the Expected Transmission Count (ETX) metric. This is one of the preferred metrics, which represents the expected number of transmissions required to successfully transmit and acknowledge a packet on a wireless link. The ETX metric was introduced in [18], and it is mathematically defined as $\text{ETX} = 1/(p_f\ p_r)$, where p_f is the measured probability that a packet is received by the neighbor and p_r is the measured probability that the acknowledgment packet is successfully received. The ETX metric is sensible to packet loss, but it is not sensible to delay. This metric is affected by two main components: the quality of the wireless channel and collisions. The RPL protocol does not assume a probe mechanism based on broadcast messages as in [18] to estimate the ETX value. Indeed, the practical implementations of RPL in Contiki operating system [19] start measuring ETX only when the unicast data traffic is actually transmitted. According to the RPL specification, the ETX value before a node initiates the data transmission is $\text{ETX} = 4$. As soon as network nodes join the DODAG, the unicast data traffic can start, which triggers the estimation of the ETX based on the number of retransmissions required to correctly deliver a data packet.

Based on simulation experiments, we propose a refined ETX estimation procedure in order to allow RPL to quickly track the link modifications. For each node link a circular buffer stores the last five number of retransmissions required to deliver the last five data packets,

$$\text{RTX}_{\text{buffer}} = \{rtx_{i-4}, rtx_{i-3}, rtx_{i-2}.rtx_{i-1}, rtx_i\}. \quad (1)$$

The ETX is updated according to the following rule

$$\begin{aligned}\text{ETX} =& 0.1 \cdot rtx_{i-4} + 0.1 \cdot rtx_{i-3} \\ &+ 0.2 \cdot rtx_{i-2} + 0.3 \cdot rtx_{i-1} + 0.3 \cdot rtx_i.\end{aligned} \quad (2)$$

This modification speeds up the DODAG construction in comparison with the default RPL implementation in Contiki. In the presence of a jammer node, the ETX metric is affected depending on the interference level. Nodes closer to the interferer will be blocked by contention because they sense the channel is busy. Other network nodes will experience a degradation on the link performance because the absence of confirmation for the transmitted packets.

V. Channel Model

The channel path loss is modeled according to the log-distance [20] propagation model,

$$P_L^{dB} = P_{L_0}^{dB} + 10\ n\ \log_{10}\left(\frac{d}{d_0}\right), \quad (3)$$

where d is the transmitter-receiver distance and n is the path loss exponent. The parameter $P_L^{dB}(d_0)$ is the free-space path loss computed at the reference distance $d_0 = 1$ m,

$$P_{L_0}^{dB} = 10\ \log_{10}\left(\frac{4\pi d_0}{\lambda}\right)^2, \quad (4)$$

where λ is the wavelength. The received power is given by

$$P_{rx}^{\mathrm{dBm}} = P_{tx}^{\mathrm{dBm}} + G_t^{\mathrm{dB}} + G_r^{\mathrm{dB}} - P_L^{\mathrm{dB}} - N_F^{dB}, \quad (5)$$

where P_{tx} is the transmit power, while G_t^{dB} and G_r^{dB} are the transmitter and receiver antenna gains, respectively. The parameter N_F^{dB} is the receiver noise figure.

In this case the average signal-to-interference-plus-noise ratio (SINR) at the receiver is

$$\overline{\gamma} = \frac{P_{rx}}{P_n + P_I + P_J} \quad (6)$$

where P_{rx} is the received signal power, $P_n = N_0 \cdot B$ is the noise power at the receiver and N_0 is the noise power spectral density in Watts/Hz. The parameter P_I represents the total interference power

$$P_I = \sum_{j \in N_I} P_{rx}^j, \quad (7)$$

where N_I is the subset of nodes in the network which are transmitting simultaneously affecting the current transmission, and P_{rx}^j is the received power from the j-th interferer node. P_J represents the power of the jammer node. Note that in this model the interferer and jamming signals are modeled as additional Gaussian noise [20].

The outage probability is an important metric for the performance evaluation of a wireless communication link because it gives a good approximation for the packet error rate (PER) caused by radio impairments, such as path loss and fading [20]. An outage occurs at the receiver when the instantaneous SINR γ is below a threshold $\beta = 2^{\Delta} - 1$ which allows error free decoding. The parameter Δ is the system spectral efficiency in bits/s/Hz and B is the system bandwidth in Hz.

In this paper we employ the Nakagami-m [20] distribution to model the multipath fading effects in the wireless channel, so that the fading severity can be adjusted through the parameter m. Moreover, the instantaneous SINR can be written as $\gamma = h^2\overline{\gamma}$, where h is the fading envelop, which is Nakagami-m distributed, and thus γ follows a gamma distribution [20]. Therefore, the outage probability for the channel model used in this paper is given by

$$\mathcal{O} = \mathbb{P}\left[\gamma < \beta\right] = \Psi\left(m, \frac{m \cdot \beta}{\overline{\gamma}}\right) / \Gamma(m), \quad (8)$$

where $\Gamma(a)$ and $\Psi(a, b)$ are the complete and lower imcomplete gamma functions.

VI. Study Case

In this section, we investigate the behavior of the RPL protocol in a multigateway AMI network in the presence of jamming attacks. We consider a wireless NAN whose smart meters and gateways are equipped with IEEE802.15.4g radios. This standard specifies a physical layer transmission scheme which is suitable for smart metering applications [21]. Particularly, we consider in our simulations the parameters of the IEEE802.15.4g AVR radio [22] operating at the 914MHz frequency. The receiver noise figure is $N_F^{dB} = 4.5$ dB and

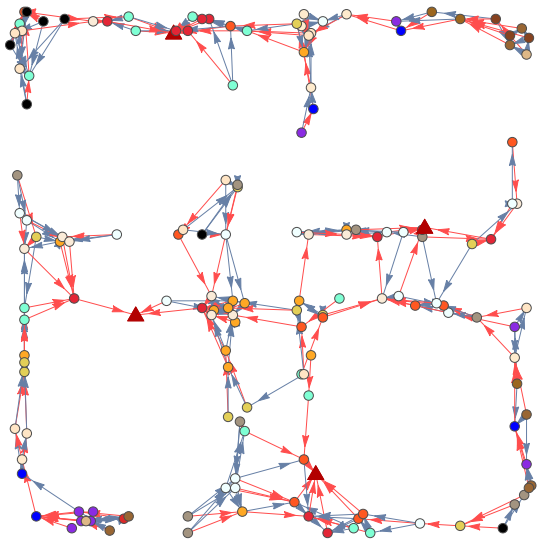

Figure 3. Example of constructed DODAG with 4 gateways.

the transmission power range is adjustable between -12 and 15 dBm. For the log-distance model, we assume a path loss exponent $n = 3.7$, which is a reasonable value for modeling path loss in dense urban areas. The antenna gains are set to $G_t^{dB} = G_r^{dB} = 0$ and the fading parameter to $m = 2$.

Furthermore, we consider NAN topologies covering four square street blocks, where each block has dimension (l, l)=$(100, 100)$ meters. The distance c of the border of the block where the smart meters can be deployed was set to 10m and the street width to 20m. We assume topologies with a density of 40 nodes per block (total of 160 nodes) and transmission power of -10 dBm for all NAN nodes. In our analysis, we consider scenarios with 2, 4 and 6 gateways. The jamming node is randomly placed in the network coverage area and uses a transmission power of 0 dBm.

We employed an ad-hoc packet simulator developed in software Mathematica, in order to implement RPL and the MAC layer with CSMA/CA, as well as the physical layer with a precise interference model. Figure 3 shows an example of the DODAG generated by the RPL for a scenario without jammer and four gateways. The gateways are indicated by a triangle, the preferred parent is represented by a red line connection, the alternative parents are represented by blue connections and node color indicates the node rank. Nodes with the same color have the same rank. All nodes employ adaptive Poisson traffic sources. The nodes adjust the average transmission rate during the network operation in order to reduce congestion and to optimize network capacity. When the network becomes congested, the DODAG construction and maintenance is affected.

The first analysis considers the case without jammer. We investigated the RPL dynamics in terms of the number of isolated nodes in the DODAG. From Figure 4 we can ver-

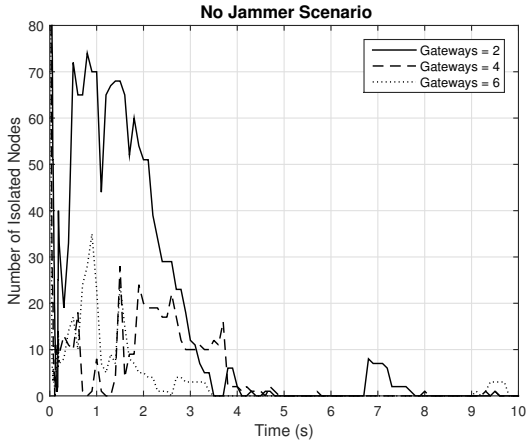

Figure 4. Number of isolated nodes in the network.

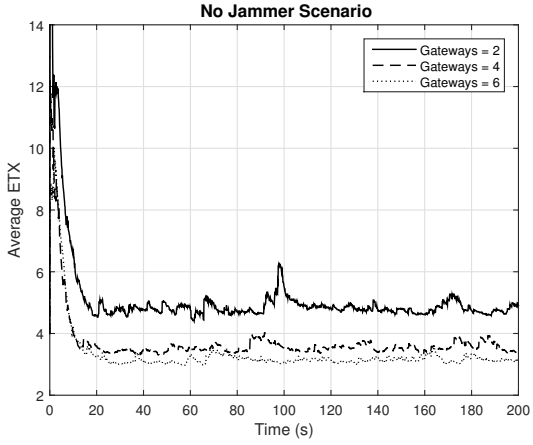

Figure 5. Average ETX of the routing paths.

ify that RPL is able to connect all nodes in less than 10 seconds. Along the network operation, we can observe the disconnection and reconnection of some nodes. This behavior is caused by two reasons. The first one is that some nodes can have poor link performance and they are more affected by the outage probability. The second one is the intraflow and interflow interference [23], which changes according to the adaptation of the traffic sources. The RPL quickly runs in the scenario with six gateways because the reduced size of the DODAGs.

Figure 5 presents the behaviour of the average ETX metric. The metric stabilizes around 30 seconds and achieves a better operating point in the scenario with six gateways because we have shorter routing paths. In the scenario with two gateways, there is a greater oscillation in the ETX metric because a node's disconnection can trigger the disconnection of a great number of descendant nodes. The scenario with four gateways performs similarly to the six gateway scenario, with a little performance degradation. The average ETX metric indicates that a good choice for number of gateways for this topological model should be between four and six gateways.

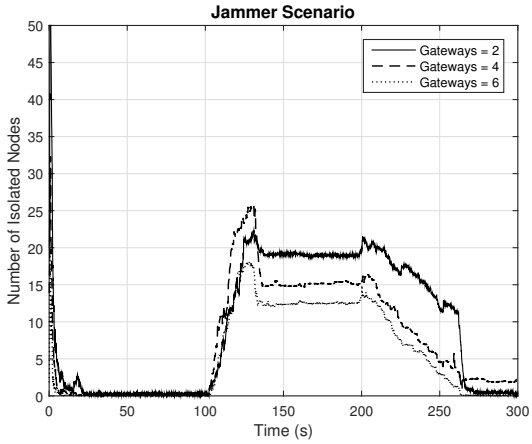

Figure 6. Number of isolated nodes in the network.

Figures 6 and 7 show the results with the presence of a jamming node. We assume that the jamming node starts transmitting at 100s and ends at 200s. This period was selected because the DODAG was already in a steady state operation. We considered an ensemble of 30 topologies and 50 random selected positions for the jammer node in each topology.

Figure 6 shows the averaged number of isolated nodes. The active period of the interferer is easily identified. We can identify three different phases in the RPL dynamics. During approximately the first 30 seconds, after the jamming signal started, the nodes severely affected become disconnected from the corresponding DODAG. Some nodes have joined to other DODAGs or they reconnected through an alternative path. The second phase corresponds to the steady state operation under jamming attack. The third phase starts when the jammer stops transmitting. We can observe from Figure 6 that the recovery time lasts for 70 seconds, approximately. This information is relevant for time-critical applications because nodes must quickly reconnect the DODAG. The reconnection time is affected by ETX estimation procedure, which can be optimized.

We can observe from Figure 7 that in both 4 and 6 gateways scenarios, the average ETX value returned to approximately the same levels. In the case of 2 gateways (density of 80 nodes/gateway), the ETX stabilized at a sligtly higher level because its structure has undergone more changes. In this case, as ETX metric is updated based on the unicast data traffic, it is necessary a much longer network operation time in order to RPL establish the DODAG to the initial configuration. Therefore, the DODAG recovery time can significantly exceed the attack period, which can compromise time-constrained applications. Based on the average ETX metric we can select the appropriated number of gateways for a specific topological model, avoiding deploying an excessive number of gateways.

Figure 8 shows a comparison considering different powers for the jammer node in a scenario with six gateways. For a jammer with the power of +15dBm, approximately 50% of the NAN nodes are compromised during the attack period.

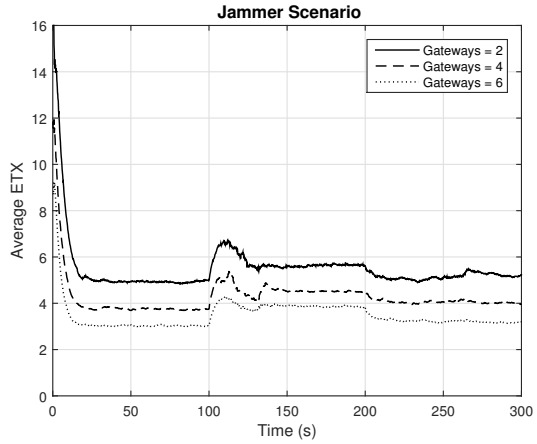

Figure 7. Average ETX of the routing paths.

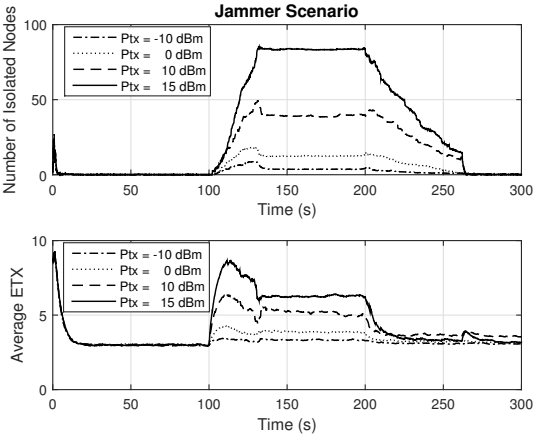

Figure 8. Influence of the jammer transmission power.

VII. Conclusions

The AMI architecture based on wireless NAN deployments is susceptible to intentional jamming attacks. The RPL has complex interactions with the network due to the link quality estimation and maintenance of the routing paths. The knowledge of the protocol dynamics under jamming attacks is an important issue because it helps to define better NAN design rules for time-critical applications. In this paper we employ a realistic topological model for the NAN and propose a refined ETX estimation procedure. The RPL dynamics under jamming attack was investigated. The results show that in NAN scenarios with a density of 80 nodes/gateway the DODAG recovery time can significantly exceed the attack period, which can compromise time-constrained applications. A jamming attack with maximum power (+15 dBm) can compromise almost 50% of the NAN nodes.

References

[1] C.-H. Lo and N. Ansari, "The progressive smart grid system from both power and communications aspects," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 3, pp. 799–821, Third 2012.

[2] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. H. Chin, "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 1, pp. 21–38, First 2013.

[3] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: a survey," *Network, IEEE*, vol. 28, no. 1, pp. 24–32, January 2014.

[4] A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "Rpl: Ipv6 routing protocol for low-power and lossy networks," *Internet Requests for Comments*, no. 6550, pp. 1–157, March 2012.

[5] E. Ancillotti, R. Bruno, and M. Conti, "Rpl routing protocol in advanced metering infrastructures: An analysis of the unreliability problems," in *Sustainable Internet and ICT for Sustainability (SustainIT), 2012*, Oct 2012, pp. 1–10.

[6] ——, "The role of the rpl routing protocol for smart grid communications," *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 75–83, January 2013.

[7] V. Kathuria, G. Mohanasundaram, and S. Das, "A simulation study of routing protocols for smart meter networks," in *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, Oct 2013, pp. 384–389.

[8] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The trickle algorithm," Internet Requests for Comments, RFC 6206, March 2011.

[9] S. Babar, N. Prasad, and R. Prasad, "Jamming attack: Behavioral modelling and analysis," in *Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2013 3rd International Conference on*, June 2013, pp. 1–5.

[10] P. Thulasiraman, "Rpl routing for multigateway ami networks under interference constraints," in *Communications (ICC), 2013 IEEE International Conference on*, June 2013, pp. 4477–4482.

[11] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *Mobile Computing, IEEE Transactions on*, vol. 13, no. 8, pp. 1746–1759, Aug 2014.

[12] K.-H. Chang and B. Mason, "The ieee 802.15.4g standard for smart metering utility networks," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, Nov 2012, pp. 476–480.

[13] U. DOE, "Communications requirements of smart grid technologies," *US Department of Energy, Tech. Rep*, pp. 1–69, 2010.

[14] A. Das and S. Das, "Cost optimization of wireless-enabled metering infrastuctures," *Wireless and Microwave Technology Conference (WAMICON), 2012 IEEE 13th Annual*, pp. 1–6, April 2012.

[15] T. Otani and M. Miyashita, "Characteristics of ami using dlms/cosem and ieee 802.15.4g multi-hop wireless communication," *Smart Grid Communications (SmartGridComm), 2013 IEEE International Conference on*, pp. 324–329, Oct 2013.

[16] S. Nowak, M. Nowak, and K. Grochla, "Properties of advanced metering infrastructure networks' topologies," in *Network Operations and Management Symposium (NOMS), 2014 IEEE*, May 2014, pp. 1–6.

[17] J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, "Routing metrics used for path calculation in low-power and lossy networks," *Internet Requests for Comments*, no. 6551, pp. 1–30, March 2012.

[18] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '03. New York, NY, USA: ACM, 2003, pp. 134–146. [Online]. Available: http://doi.acm.org/10.1145/938985.939000

[19] C.-M. Tang, Y. Zhang, and Y.-P. Wu, "The p2p-rpl routing protocol research and implementation in contiki operating system," in *Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2012 Second International Conference on*, Dec 2012, pp. 1472–1475.

[20] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[21] K.-H. Chang and B. Mason, "The ieee 802.15.4g standard for smart metering utility networks," *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, pp. 476–480, 2012.

[22] *Atmel AT86RF215 Device Family*, Atmel Corporation, 7 2015, rev. 1.0.

[23] M. Boushaba, A. Hafid, and M. Gendreau, "Source-based routing in wireless mesh networks," *Systems Journal, IEEE*, vol. PP, no. 99, pp. 1–9, 2014.