A Resilient Dynamic Gateway Selection Algorithm Based on Quality Aware Metrics for Smart Grids

Vitor Hugo Okabayashi
Federal Fluminense University
vhugo@ic.uff.br

Igor Ribeiro
Federal Fluminense University
iribeiro@ic.uff.br

Diego Passos
Federal Fluminense University
dpassos@ic.uff.br

Célio Albuquerque
Federal Fluminense University
celio@ic.uff.br

ABSTRACT

Smart Grid represents the evolution of the current electrical power system. It is designed to meet the challenge of increasing demands for energy by fully integrating the electrical power grid with data communication networks. One of the main challenges faced by this kind of network is to fulfill reliability and resilience requirements in order to meet various types of services and applications. Wireless mesh networks can provide scalability and resilience to this communication network, but there are issues that need to be addressed before it can be used in practical smart grids. One of these issues relates to the robustness of the network when it faces gateway failures. In this situation, communication to smart meters may be unavailable for a considerable amount of time, which is prohibitive for many types of applications. In this sense, we present DDSA, an algorithm for dynamic selection of gateways in a multihoming smart grid network. The algorithm uses a probabilistic approach for choosing gateways, prioritizing those with the most reliable paths. Results indicate that DDSA increases network robustness and resilience in the presence of gateway failures compared to existing algorithms for dynamic gateway selection.

Categories and Subject Descriptors

C.2 [**COMPUTER-COMMUNICATION NETWORKS**]: General

Keywords

Smart Grids; Advanced Metering Infrastructure; AMI; Reliability

1. INTRODUCTION

The current electrical power system architecture does not meet the future demands of energy consumption, presenting a number of shortcomings such as: low and deficient communication and reliability problems [9]. Smart Grids represent an evolution of the existing electrical power system and aims at solving these inefficiencies, departing from the current model of one-way flow and deploying a two-way flow for energy and communication [9, 19]. A two-way communication network is essential for smart grids, supporting the sending of commands and the gathering of information from components and sensors in real time, allowing monitoring, maintenance and control [12].

The Advanced Metering Infrastructure (AMI) is a fundamental component of a smart grid, and it is the first step in its deployment [1, 17, 18]. The AMI is basically composed of smart meters, which collect data such as energy consumption of the equipment inside a residence and Data Aggregation Points (DAPs) that act as gateways to forward data from smart meters to the utility's headend and commands from the headend to the smart meters. In order for a smart grid to work properly, the AMI communication network must meet some strict requirements regarding its reliability, latency and response time to each application [12].

Communication in smart grids may use available wired or wireless technologies that support the exchange of information between components of the AMI [6, 24]. Different types of technologies can be used: cellular technology [22], ZigBee [22], RF Mesh [15], IEEE 802.11-based Wireless Mesh Networks (WMN) [2] and Power Line Communication (PLC) [16]. PLC is a promising wired technology, but it has limitations. In case of failures, such as physical disruption of power lines, it would not be possible to maintain communication between AMI components [11]. Wireless networks offer more benefits than wired networks, such as lower cost, ease of deployment and signal availability in large areas [22].

Among all wireless technologies, WMN has advantages compared to single-hop infrastructured network architectures since it communicates in a multi-hop fashion, what extends the coverage of the network and allows communication with alternative paths in case of failures [8,15]. However, the WMN must be adapted to the communication requirements of AMI. Typically, an AMI is composed of a communication network connecting smart meters within a given neighborhood to a specific single DAP. Each DAP is connected to the utility's headend through the network's backbone.

In this architecture, in case of DAP failure, the associated smart meters become temporarily disconnected from the utility's headend, therefore failing to meet AMI's availability and reliability requirements. To overcome this problem, we propose the Dynamic DAP Selection Algorithm (DDSA). Assuming that each meter can reach multiple DAPs through one or more hops, DDSA maintains a set of reachable DAPs that provides the best path metrics. When a smart meter needs to send a packet, DDSA randomly selects one DAP from the list and route the packet through this selected DAP. The main goal of DDSA is to allow smart meters to use multiple DAPs, therefore increasing network's robustness and resiliency.

The contributions of this paper are three-fold:

- Proposal of DDSA, an algorithm that improves the resiliency and robustness of an AMI network in the presence of DAP failures;
- Mathematical analysis of an algorithm that always selects the DAP to which the routing metric is the best possible. Throughout this paper, we call this algorithm Best_ETX;
- Mathematical model of DDSA and its comparison against the Best_ETX algorithm.

The remaining of this paper is organized as follows. Section 2 presents the related works. Section 3 provides a mathematical analysis of the Best-ETX algorithm in a scenario with a DAP failure. In Section 4 we present the proposed DDSA algorithm. In addition, a mathematical model of DDSA configured with the ETX routing metric is presented and compared against the Best-ETX model. Simulation results are discussed in Section 5, and Section 6 concludes the paper and presents future works.

2. RELATED WORK

One class of proposals uses a single DAP to implement AMI networks [11, 15]. The work in [11] proposes the use of WMN where multiple domains of mesh networks are connected by a WiMAX backbone. This architecture provides redundant paths between smart meters mitigating problems like broken routes due to node failure increasing their resilience. However, this work considers only one DAP acting as gateway in each WMN domain. If it becomes unavailable, there will be no communication between smart meters and the headend. This is the same problem studied by [15] where the WMN consists of smart meters, routers and collectors. The smart meters communicate with routers or directly to collectors, and the latter controls up to 25,000 smart meters and routers on a single network.

The second class of proposals uses multiple DAPs in the AMI network [5, 10, 14]. The work in [5] makes use of multiple gateways to increase WMN resilience because in addition to providing redundant paths, it also provides gateway redundancy. This approach is applied to WMN that serves as the backbone for Internet access but uses only the gateway with the best path.

The works in [14] and [10] are designed to meet the requirements of AMI networks and make use of multiple DAPs for communication between smart meters and headend, modifying the HWMP protocol (Hybrid Wireless Mesh Protocol). Although the work in [10] solves some deficiencies of the HWMP protocol, it still suffers from other problems such as route instability and loops. According to the authors, this is a characteristic of the distributed backpressure system adopted by them. However, neither of them has evaluated the protocol behavior in an environment with DAP failures nor allowed transmission rate adaptation, which increases the problem of route instability. They use a base protocol that has scalability problems due to the congestion caused by control messages [3] making it difficult to use in AMI.

Our proposal, DDSA, makes use of multiple DAPs for communication between smart meters and the utility's head-end and differs from [14] and [10] because it is designed to improve performance in environments with DAP failures. DDSA is independent from the routing protocol. Moreover, it can be implemented in a protocol that best suits the implementation of the AMI.

3. MOTIVATION

In the Advanced Metering Infrastructure, all smart meters must be able to communicate with at least one DAP. The AMI imposes strong requirements on the communication network in terms of reliability and latency. However, due to the unstable nature of the wireless networks and to the fact that the network equipment is deployed in public venues (and, thus are vulnerable to accidents, attacks and natural disasters), it is imperative to employ a routing protocol robust enough to maintain good performance even in case of DAP failures.

Ideally, in a WMN-based AMI, smart meters can reach multiple DAPs directly or through multi-hop paths. However, typical WMN routing protocols select a single DAP (i.e., the closest one according to the routing metric). If the selected DAP fails, the associated smart meters become disconnected. The amount of time in which the smart meters will remain disconnected depends on the time the metric takes to reflect the failure and the time needed for the route update to propagate throughout the network.

To better understand the implications of a DAP failure in the Smart Grid, lets consider the scenario in which smart meter A (called node A henceforth) directly reaches DAPs B and C through links $(A-B)$ and $(A-C)$, respectively. To improve performance, it is important to use a routing metric that considers the path quality. Hence, in this example we use the Expected Transmission Count (ETX) as the routing metric.

The ETX of a link represents the expected number of link layer transmissions until a packet is successfully delivered to the destination. In fact, ETX only considers a packet to be successfully delivered through a link if it has been received by the destination and the corresponding acknowledgment from the destination is also correctly received by the source. From the perspective of node A, the ETX in the link $(A-B)$ in a given time t can be calculated according to Equation 1, where $d_f(t)^{A\to B}$ is the probability the packet is successfully received by its destination (forward direction) and $d_r(t)^{B\to A}$ is the probability the ack is successfully received by the source (reverse direction).

$$ETX(t)^{A-B} = \frac{1}{d_f(t)^{A\to B} \cdot d_r(t)^{B\to A}} \tag{1}$$

In order to calculate the ETX metric, nodes A and B send probe packets every T seconds. They keep track of all probes received during the current time window W, which can contain at most $\frac{W}{T}$ probes. Consequently, each node can easily calculate the probability of successful delivery of a packet in the reverse path. Specifically, node A can calculate

$d_r(t)^{B \to A}$ using Equation 2, where $C_B(t)$ is the number of probes node A correctly received from DAP B in the current time window. However, node A does not know how many of its probes to DAP B were successfully received. Therefore, node A must retrieve this information from DAP B in order to calculate $d_f(t)^{A \to B}$. Hence, every probe sent from DAP B to node A contains the number of probes sent from A and received by DAP B in the current time window.

$$d_r(t)^{B \to A} = \frac{C_B(t)}{\frac{W}{T}} \tag{2}$$

Now, lets consider that when node A needs to send some data to the utility's headend, it always selects the DAP that provides the path with the best (lowest) ETX metric among all reachable DAPs. From now on we call this algorithm Best_ETX. Suppose that at time t_0, $ETX(t_0)^{A-B} < ETX(t_0)^{A-C}$. Consequently, all packets sent by node A to the utility's headend are routed through DAP B. Moreover, the delivery probability of the link $(A - B)$ is given by $\frac{1}{ETX(t_0)^{A-B}}$. In order to make the analysis simpler, we assume $ETX(t)^{A-C} = ETX(t_0)^{A-C}, \forall t$.

Now, suppose that at time t_f DAP B fails and stops working. Consequently, DAP B stops sending probes, making it impossible for node A to correctly learn new values of $d_f(t)^{A \to B}$. Hence, we consider $d_f(t)^{A \to B} = d_f(t_f)^{A \to B}$ for $t \geq t_f$[1]. In addition, because node A stops receiving probes from DAP B, the value of $C_B(t)$ decreases with time. In fact, after every T seconds, the ETX time window W shifts one position to the right. At this time, if the leftmost probe of W sent by DAP B has been correctly received by node A, $C_B(t)$ is reduced by one. However, if the leftmost probe in W sent by DAP B has not been correctly received by node A, $C_B(t)$ remains the same. Approximating each entry of the ETX time window by its expected value, we obtain Equation 3.

$$C_B(t) = C_B(t_f) - \frac{C_B(t_f)}{\frac{W}{T}} \cdot \frac{(t - t_f)}{T}, t > t_f \tag{3}$$

After W seconds, the ETX window of the link $(A-B)$ will become completely empty. At this time, which we call t_{end}, $d_r(t_{end})^{B \to A} = 0$ and, consequently, $ETX(t_{end})^{A-B} = \infty$. Hence, after time t_{end}, the link $A - B$ is considered broken and node A will have no alternative but to route packets through DAP C. Notice, however, that DAP C will be chosen by node A before t_{end}, namely at time t_{eq}, where $t_f < t_{eq} < t_{end}$ and $ETX(t_{eq})^{A-B} = ETX(t_{eq})^{A-C} = ETX(t_0)^{A-C}$.

$$Prob_{etx}(t) = \begin{cases} \frac{1}{ETX(t_f)^{A-B}} & t \leq t_f \\ 0 & t_f < t < t_{eq} \\ \frac{1}{ETX(t_f)^{A-C}} & t \geq t_{eq} \end{cases} \tag{4}$$

Equation 4 summarizes the behavior of Best_ETX algorithm in the previous example scenario in terms of packet delivery probability between node A and its chosen DAP. It can be observed that before the recovery time $T_{rec} = (t_{eq} - t_f)$ the delivery probability is zero. Since availability is very important for AMI applications, T_{rec} provides a good measure of the network performance in case of DAP failures. Notice that T_{rec} can be derived by applying Equation 3 to Equations 2 and 1, as shown in Equation 5.

$$T_{rec} = W \cdot \left(1 - \frac{ETX(t_f)^{A-B}}{ETX(t_f)^{A-C}}\right), t > t_f \tag{5}$$

Consider the following numerical example. Let $d_f(t_f)^{A \to B} = d_r(t_f)^{B \to A} = 0.9$ and $d_f^{A \to C} = d_r^{C \to A} = 0.6$. Therefore, we have $ETX(t_f)^{A-B} = 1.23$ and $ETX(t_f)^{A-C} = 2.78$. Every node sends one probe per second ($T = 1s$) and is configured with $W = 100s$. Suppose that DAP B fails at time $t_f = 20s$. Applying these parameters to Equation 5 results that no packets sent by node A are received by any DAP for approximately $56s$. Considering that some AMI applications have latency restrictions of about $2s$ [13], this scenario becomes undesirable.

In fact, this scenario is an optimistic one. Consider now that node A is connected to DAPs B and C through multiple hops. In this case, when DAP B fails, the changes in the ETX metric are not directly perceived by node A. Instead, this information must be propagated back by the routing protocol as a route update. Hence, in a multihop scenario, the recovery time T_{rec} can be much greater than the value calculated through Equation 5.

4. DYNAMIC DAP SELECTION ALGORITHM (DDSA)

The idea behind the Dynamic DAP Selection Algorithm (DDSA) is to leverage the existence of multiple DAPs to improve network resilience in case of failures. A naive approach could lead to a simplistic solution in which the sending node replicates all packets and sends a copy to each reachable DAP. In this case, the delivery probability would be, in principle, maximized. However, since typical wireless technologies employed in WMN (such as 802.11) are contention-based, flooding all packets to all DAPs could result in an excessive number of collisions, increasing latency and degrading network performance.

As an alternative solution, the sending node could probabilistically choose a destination DAP each time it needs to send a packet. However, the efficiency of this solution depends highly on the way in which probabilities are assigned to DAPs. For example, if we suppose that the probabilities are uniformly distributed over all DAPs, then all of them would be equally likely to be selected, regardless of their respective path quality. In other words, if DAP A presents the best possible path metric and all other DAPs present the worst possible path metric, the sending node would select the best DAP with probability $\frac{1}{N}$, while the worst DAPs would be selected with probability $\frac{(N-1)}{N}$. Clearly, this approach is very inefficient. We can therefore conclude that the assignment of probabilities to DAPs must consider the path metric in order to give higher probabilities to better DAPs. Therefore, we argue that the routing metric must be quality aware and must handle varying link rates.

The proposed Dynamic DAP Selection Algorithm (DDSA) is based on a randomized algorithm triggered by two events: *Topology Update* and *Send Data*.

[1] In fact, routing protocols often associate an validity property to $d_r(t)^{B \to A}$ and $d_f(t)^{A \to B}$ in such a way that if the current value of $d_r(t)^{B \to A}$ or $d_f(t)^{A \to B}$ is older than the validity property, the value is discarded. However, for our purposes, we consider that all calculations performed in this section occur in a time frame shorter than any validity property.

4.1 Topology Update

When routing information is updated in smart meter m_i, DDSA recalculates the selection probability for all reachable DAPs. This task can be accomplished in two different ways depending on the behavior of the routing metric being used. If the routing metric assigns higher values to better quality links, the selection probability of DAP d_j is given by Equation 6. On the other hand, if the routing metric assigns lower values to better quality links, Equation 7 is used instead. In both equations, $M(m_i, d_k)$ represents the cost of the best path from smart meter m_i to DAP d_k and N is the number of reachable DAPs. Consequently, when smart meter m_i needs to send a data packet, it chooses DAP d_k with probability $P(m_i, d_k)$.

$$P(m_i, d_j) = \frac{M(m_i, d_j)}{\sum_{k=1}^{N} M(m_i, d_k)} \tag{6}$$

The selection probability assignment process provided by equations 6 and 7 allows us to select better DAPs more often. However, in some cases, the value $M(m_i, d_j)$ for some DAP d_j may be too low (or too high), what makes DAP d_j useless in practice. Even so, some packets would still be sent to DAP d_j because the selection probability $P(m_i, d_j)$ is not zero. This problem can reduce the overall delivery probability of DDSA.

$$P(m_i, d_j) = \frac{1/M(m_i, d_j)}{\sum_{k=1}^{N} 1/M(m_i, d_k)} \tag{7}$$

Algorithm 1: Exclude DAP with Cost Below Threshold.

```
1  d_best ← find_best_dap()
2  P(m_i, d_best) ← get_selection_probability(m_i, d_best)
3  γ ← α · P(m_i, d_best)
4  discarded ← FALSE
5  for each DAP d_k do
6      P(m_i, d_k) ← get_selection_probability(m_i, d_k)
7      if P(m_i, d_k) < γ then
8          P(m_i, d_k) ← 0
9          discarded ← TRUE
10     end
11 end
12 if discarded then
13     recalculate_selection_probabilities()
14 end
```

To overcome this problem, DDSA executes Algorithm 1, which discards all DAPs d_k whose $P(m_i, d_k)$ is below a threshold. First, the algorithm finds the DAP d_{best} such that $M(m_i, d_{best})$ has the best value considering all other reachable DAPs (line 1). Next, the algorithm retrieves the selection probability for DAP d_{best} (line 2). This process is straightforward because DDSA has already calculated and stored the selection probability to all reachable DAPs.

In the next step, Algorithm 1 calculates the value of the threshold γ (line 3). In order to do so, the user must configure the value of parameter $\alpha \in [0, 1]$. This choice must be done carefully, because higher values of α result in the use of better DAPs at the price of reducing resilience in case of DAP failures. Then, the algorithm discards all DAPs d_k such that $P(m_i, d_k) < \gamma$ (lines 5 through 11). Finally, if any DAP was discarded, then the selection probability for all remaining DAPs must be recalculated (line 13). Notice that recalculate the selection probabilities means to calculate the summation in the denominator of Equation 6 or Equation 7 considering every DAP d_k that was not excluded by the Algorithm 1.

4.2 Send Data

The Send Data event is triggered whenever a smart meter needs to send information to the utility's headend. DDSA keeps a table containing the assigned selection probability for all reachable DAPs. Consequently, when smart meter m_i needs to send a packet, it chooses DAP d_k with probability $P(m_i, d_k)$. Note that if the DAP d_k was excluded by Algorithm 1, it will never be selected because $P(m_i, d_k) = 0$.

Algorithm 2: DAP Selection

```
1  Prob_Sum ← 0
2  rand ← randomUniform(0, 1)
3  for each DAP d_k do
4      P(m_i, d_k) ← get_selection_probability(m_i, d_k)
5      Prob_Sum ← Prob_Sum + P(m_i, d_k)
6      if Prob_Sum >= rand then
7          Selected_DAP ← d_k break
8      end
9  end
10 return Selected_DAP
```

Algorithm 2 shows the steps of the DAP selection process. First, the algorithm randomly chooses a value between 0 and 1 (line 2). Next, for each reachable DAP d_k, the algorithm retrieves de probability $P(m_i, d_k)$ and sums it to variable $Prob\_Sum$ (lines 4 and 5). These steps are repeated until $Prob\_Sum$ is greater than or equal to the selected value $rand$, in which case the current DAP is chosen as the gateway for this specific application message (lines 6 through 8). It's worth mentioning that the list of DAPs is not sorted by cost nor by selection probability, which could influence the result of the DAP selection process.

4.3 Comparing DDSA with Best_ETX

Before we move to Section 5, let's analyze how DDSA compares to Best_ETX in the scenario explained in Section 3. In this analysis, we assume that DDSA operates using the ETX metric. Because greater values of ETX indicate worse links, we must use Equation 7 to calculate the selection probability, resulting in Equation 8. Note that, as already said, we consider $ETX(t)^{A-C} = ETX(t_f)^{A-C}, \forall t$.

$$P(t)^{A-B} = \frac{ETX(t_f)^{A-C}}{ETX(t_f)^{A-C} + ETX(t)^{A-B}} \tag{8}$$

Before time t_f, when DAP B fails, node A sends packets to DAP B with probability $P(t)^{A-B}$ and to DAP C with probability $P(t)^{A-C}$. Once a packet is destined to DAP B, it is correctly delivered with probability $\frac{1}{ETX(t_f)^{A-B}}$. Similarly, once a packet is destined to DAP C, it is correctly delivered with probability $\frac{1}{ETX(t_f)^{A-C}}$. When DAP B fails, all packets sent to it are lost. However, some packets are still destined to DAP C and some of them are correctly delivered. After W time units from time t_f ($t_{rec} = t_f + W$), we get $ETX(t_{rec})^{A-B} = \infty$. Consequently, DAP B's selection probability becomes zero. From this time onward, all packets start to be routed through DAP C. Equation 9 summarizes this scenario in terms of the delivery probability of a packet.

$$Prob(t)_{ddsa} = \begin{cases} P(t)^{A-B} \cdot \frac{1}{ETX(t_f)^{A-B}} + & \\ P(t)^{A-C} \cdot \frac{1}{ETX(t_f)^{A-C}} & t \leq t_f \\ P(t)^{A-C} \cdot \frac{1}{ETX(t_f)^{A-C}} & t_f < t < t_{rec} \\ \frac{1}{ETX(t_f)^{A-C}} & t \geq (t_{rec}) \end{cases} \tag{9}$$

Notice, however, that in a typical WMN, a link-layer protocol such as 802.11 MAC will provide up to M retransmissions of unicast frames, resulting in higher delivery probabilities, according to Equation 10, where $Prob(t)$ is the probability a packet is correctly received in time t.

$$Prob_{retrans}(t) = 1 - (1 - Prob(t))^M \tag{10}$$

Table 1: Parameters of the numerical example.

W	100 s
T	1
$ETX(t_f)^{A-B}$	1.23
$ETX(t_f)^{A-C}$	2.78
t_f	20 s

In order to compare the behaviors of Best_ETX and DDSA, we will use the same parameters used in the numerical example in Section 3. These parameters are summarized in Table 1. After calculating $Prob_{etx}(t)$ (Equation 4) and $Prob_{ddsa}$ (Equation 9(t)), we applied the results to parameter $Prob(t)$ in Equation 10 and defined $M = 4$ (the default value for 'large" frames in the 802.11 MAC).

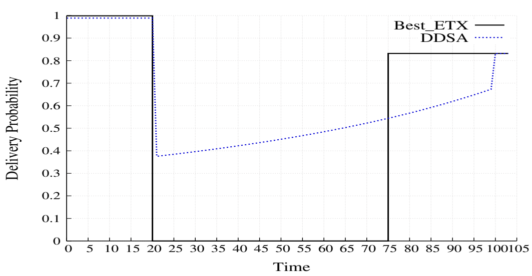


Figure 1: Example Scenario.

In Figure 1 we can observe that before DAP B fails (time $20s$) the delivery probabilities for both Best_ETX and DDSA are close to 100%. In fact, Best_ETX provides a slightly greater delivery probability than DDSA. When DAP B fails, the delivery probability considering Best_ETX falls instantly to zero and maintains this value until time $75s$, when $ETX(75)^{A-B} = ETX(75)^{A-C}$. On the other hand, DDSA presents a much better behavior. At time $20s$ the delivery probability falls rapidly to approximately 40% and continually grows until time $100s$.

Before DAP B fails, most of the packets were being sent to it. Consequently, when it failed, all these packets were lost, what made the delivery probability instantly drop. After that, as the ETX to DAP B increases, its selection probability decreases, what causes more packets to be addressed do DAP C instead of DAP B. At time $75s$, the delivery probability considering Best_ETX instantly grows to approximately 83%, which corresponds to the inverse of the ETX to DAP C, and maintains this value since forth. However, because DDSA keeps sending some packets to DAP B, its delivery probability continues to increase, but remains below the delivery probability of Best_ETX until time $100s$.

Finally, at time $100s$ the ETX to DAP B reaches infinity and its selection probability drops to zero. From this point onward the curves of Best_ETX and DDSA are coincident. Clearly, the DDSA algorithm provides better robustness in the presence of DAP failures, delivering more packets in average in the presence of DAP failures.

5. PERFORMANCE EVALUATION

5.1 Simulation Environment

In order to evaluate the performance of DDSA in the AMI layer of a smart grid, we set up the simulation environment shown in Figure 2 in the ns-2 simulator [21]. In this topology, there are thirty six smart meters arranged in a grid and three DAPs. All the nodes are supposed to operate in a suburban external scenario, which was simulated using the shadowing propagation model according to [20].

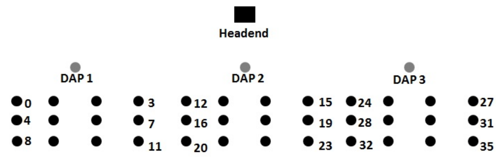


Figure 2: Scenario used in the simulation.

To simulate the exchange of information between smart meters and DAPs in a typical AMI application, a Constant Bit Rate (CBR) UDP traffic was used with fixed packet size of 400B at a rate of 1 packet at 3 seconds. Although UDP does not provide reliable transmission of data, it has some advantages over TCP, such as its lower latency, which is important for many smart grid applications. On the other hand, typical AMI applications require a high degree of reliability, which is not provided by UDP. To solve this problem, we employed a protocol at the application layer running on top of UDP that implements its own transport service suitable for AMI traffic [7]. This protocol uses a proactive retransmission strategy in which, for each generated data packet, 10 replicas are transmitted simultaneously. If any of the replicas reaches one of the DAPs, the original packet is considered to be successfully delivered. Therefore, the results regarding packet delivery rate reported in this section are calculated considering the point of view of the application layer.

As already explained, the type of routing metric used is an important factor in the DDSA performance. Consequently, in the simulations presented in this section, the routing protocol OLSR [4] was used in conjunction with the routing metric MARA [23], which estimates the path delay and performs rate adaptation. The smart meters start to send data at time 150s and at time 300s DAP 2 fails. We performed ten simulation rounds, each lasting for 650 seconds and configured with a different seed. Finally, all averages are presented with their respective 95% confidence intervals.

Lets consider now the influence of the parameter α in our simulation scenario. We evaluated two configurations of DDSA, one with a low value of α (30%) and the other with a high value of α (80%). In addition, we also compared the results from DDSA against the algorithm proposed by [5], which we call Multi-DAP henceforth. This algorithm dynamically selects the best DAP according to its path routing metric at the time the data packet is transmitted by its source node. The evaluated configurations are summarized in the following list.

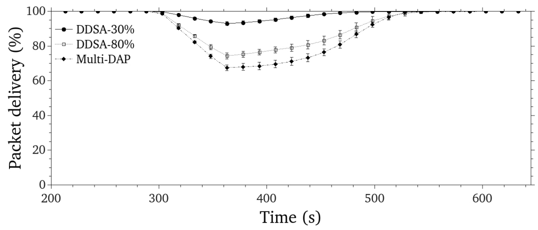
(1) DDSA with $\alpha = 0.3$ referred to as DDSA-30%;

(2) DDSA with $\alpha = 0.8$ referred to as DDSA-80%; and

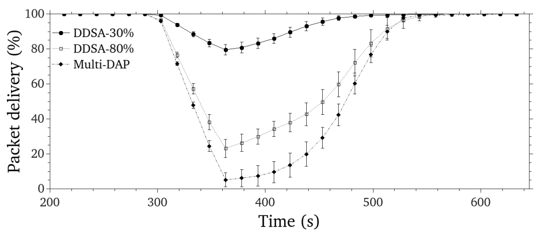
(3) Multi-DAP.

5.2 Simulation Results

Figure 3(a) shows the packet delivery ratio for all nodes as a function of time, considering the average of the latest 60 seconds. It is noticeable that the performance of DDSA-30% is higher than the other proposals after the occurrence of a DAP failure. At time 363s DDSA-30% sustains a delivery ratio of 93%, while DDSA-80% reaches 73% and Multi-DAP only 67%, what shows that DDSA-30% is less affected by the failure of the DAP 2. Particularly, Figure 3(b) shows that after the failure of DAP 2 (time 363s), DDSA-30% provides 80% of packet delivery ratio, while DDSA-30% and Multi-DAP provide only 23% and 5%, respectively, considering the central region of the network (nodes 12 to 23).



(a) Packet delivery for all nodes



(b) Packet delivery for nodes 12-23

Figure 3: Packet delivery rates as a function of time.

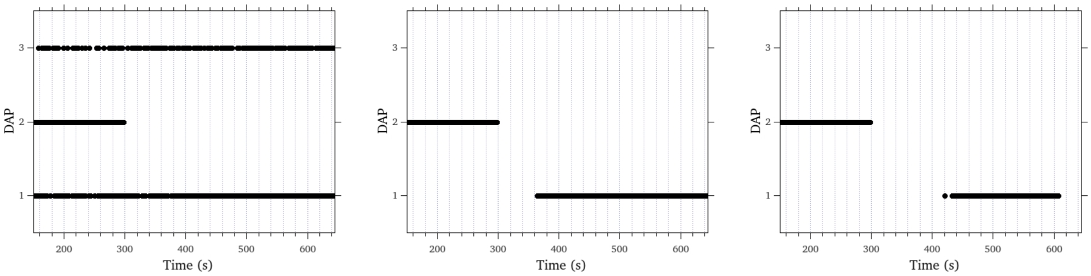
From the graphics in Figure 3, we can conclude two important facts. First, the design choice of distributing packets among DAPs (instead of choosing a single DAP) makes the data collection more robust and resilient in face of failures. Second, the value of α is crucial in the performance of the algorithm. The choice of its value represents an important trade-off, where lower values increase the reliability of the network, but also make the algorithm choose DAPs with lower quality paths. On the other hand, choosing higher values of α makes the algorithm choose DAPs with the best path qualities, but also reduces the network reliability in case of DAP failures, which can be observed by the results achieved by DDSA-80%.

To better understand how the behavior of DDSA differs from the behavior of Multi-DAP in terms of DAP selection, Figure 4 shows the choices made by node 16 using the three evaluated proposals during one round of simulation (same seed). With Multi-DAP, Before DAP 2 fails, node 16 sent all packets to DAP 2 because it has the best quality path. However, when DAP 2 fails (at 300 seconds), node 16 takes 123 seconds to employ an alternative DAP. During this period, all packets sent by note 16 are lost, what is illustrated by the gap in Figure 4(c). On the other hand, even before the failure, DDSA-30% already distributed traffic more evenly between DAPs. Consequently, when DAP 2 fails, node 16 is able to shortly recover sending its packets to DAPs 1 and 3. This behavior can be noted in Figure 4(a), where no gaps can be observed.

When we increase the value of α, the DAPs with the worse path metrics are excluded. Since in our simulation scenario there are only three available DAPs, we noticed that nodes in the center of the network (i.e., closer to DAP 2) would frequently discard DAPs 1 and 3 when $\alpha = 80\%$. That can be seen in Figure 4(b) by the existence of a gap similar to that of Figure 4(c), although shorter. After about 66 seconds, node 16 realizes that the new metric to DAP 2, although still better than the metric to the two other DAPs, is not low enough to causes DAP 1 to be excluded (refer to line 3 of Algorithm 1). From this point onward, the probability of DDSA selecting DAP 1 increases as the metric to DAP 2 decreases. Eventually, DAP 1 becomes the best DAP and DAP 2 is excluded.

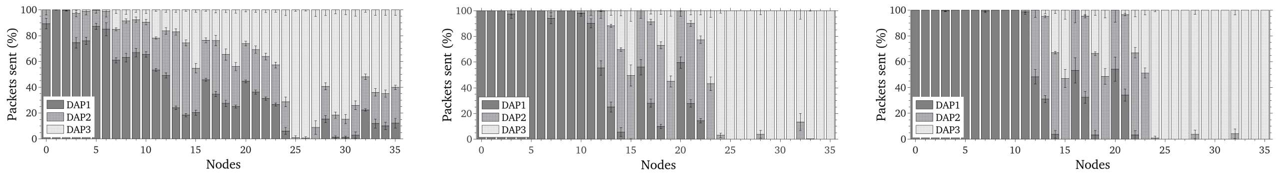
The behavior of node 16 gave us a good insight regarding the performance of the DDSA algorithm and the impact of the value of α. However, this behavior depends on the position of the node in the grid. Consequently, Figure 5 expands the analysis done in Figure 4 including all nodes (smart meters). Note that DDSA-30% (Fig. 5(a)) has a much more balanced DAP selection than the other proposals. For nodes in the central region of the network, with DDSA-30%, the lowest usage percentage is 16.4%. For Multi-DAP (Fig. 5(c)), six nodes (nodes 12, 15, 16, 19, 20, 23) only use two DAPs. Except by nodes 13 and 14, in DDSA-30% all usage percentages in the central region are below 41.6% for DAP 2 (the preferable DAP for that region). For DDSA-80%, all values are above 40.2% and for Multi-DAP they are above 45.7% for DAP 2. This demonstrates that DDSA-30% distributes packets more evenly among DAPs in the central region of the network, improving the resilience against DAP failures.

Figure 6 shows the unavailability period τ for each node with respect to the utility's headend, *i.e.*, the sum of the periods during which each node could not reach the headend through any DAP. It is clear that the long gap to deliver new packets is not unique for node 16. This behavior is repeated



(a) DDSA-30% (b) DDSA-80% (c) Multi-DAP

Figure 4: Packets received by DAP from node 16.



(a) DDSA-30% (b) DDSA-80% (c) Multi-DAP

Figure 5: Percentage of DAP usage by each node.

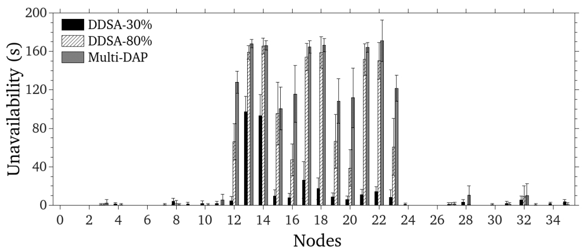


Figure 6: Unavailability Period.

for other nodes in the central region of the network as well. For DDSA-80% and Multi-DAP, these nodes suffered long periods of unavailability, while DDSA-30% sustained lower values of τ.

Nodes 13 and 14 are the closest ones to the failed DAP 2, thus suffering more influence of this failure (because their path cost to DAP 2 is much lower than the cost to other DAPs). Except for these nodes, the average unavailability period τ_{avg} for the DDSA-30% is 4.2 seconds and the maximum unavailability period τ_{max} is 26.2 seconds. For DDSA-80%, τ_{avg} is 29.5 seconds and τ_{max} is 158.8 seconds, and for Multi-DAP τ_{avg} is 40.7 seconds and τ_{max} is 166.4 seconds.

6. CONCLUSION AND FUTURE WORK

This work presented DDSA, a dynamic DAP selection algorithm to increase the reliability and resilience of AMI applications through the use of multiple DAPs in Smart Grids where the nodes are connected by a Wireless Mesh Network. In this kind of network, the DAP has an important role in the exchange of information between the smart meter and the utility's headend, because all traffic flows through it. A failure in a DAP inhibits the exchange of information on the AMI network, so alternative routes through other DAPs should be used after failure to allow the communication to happen.

First, we motivated our proposal through a mathematical analysis of the behavior of an algorithm that always selects the DAP with the best ETX metric (Best_ETX) in face of DAP failures. We shown that the selection of a single DAP, the one that presents the best metric, is problematic in case of DAP failures, causing some affected nodes to be disconnected from the utility's headend for a long period of time, reducing the delivery ratio of the overall system. In the case of Best_ETX, we provided an equation that can be used to calculate how long a node remains disconnected from the utility's headend in case of a DAP failure. After presenting the details of DDSA, we also developed a mathematical model of the algorithm, considering its use in conjunction with the ETX metric. We then compared this model with Best_ETX algorithm and showed that DDSA presents a better reliability, providing a higher overall delivery ratio.

Finally, we performed simulations to evaluate the performance of DDSA in face of DAP failures. We compared three different configurations: the DDSA algorithm with the parameter $\alpha = 0.3$, the same algorithm but with $\alpha = 0.8$ and an algorithm that always selects the DAP with the best metric (Multi-DAP). Comparing these configurations, our conclusions are two-fold:

1. DDSA improves the network reliability when a DAP fails compared to the Multi-DAP algorithm;

2. Lower values of α increase the robustness of the network, but also causes the selection of worse DAPs, what can negatively influence other network parameters, such as latency.

For future work we intend to conduct a deeper analysis of the impact of the α parameter in order to properly adjust it to provide good resilience while sustaining acceptable levels of performance. In addition, We intend to investigate the usage of a dynamic α, which automatically adapts to the ongoing network conditions. In addition, we expect to analyze the impact of other routing metrics on the performance of DDSA.

7. ACKNOWLEDGMENTS

This research was supported in part by grants from CNPq, CAPES, FAPERJ and CELESC/ANEEL (Brazil).

8. REFERENCES

[1] C. Bennett and D. Highfill. Networking AMI smart meters. In *IEEE Energy 2030 Conference.*, 2008.

[2] M. Campista, P. Esposito, I. Moraes, L. Costa, O. Duarte, D. Passos, C. de Albuquerque, D. Saade, and M. Rubinstein. Routing metrics and protocols for wireless mesh networks. *IEEE Network*, 22(1):6–12, 2008.

[3] R. Carrano, L. Magalhães, D. Saade, and C. Albuquerque. IEEE 802.11s multihop MAC: A Tutorial. *IEEE Communications Surveys & Tutorials*, 13(1):52–67, 2011.

[4] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot, et al. Optimized link state routing protocol (OLSR). *RFC 3626, Oct.*, 2003.

[5] C. da Silva, D. Passos, J. Duarte, I. Moraes, and C. Albuquerque. Dyntun: A tool for providing multihoming support in wireless mesh networks. In *International Information and Telecommunication Technologies Symposium*, 2010.

[6] G. Deconinck. An evaluation of two-way communication means for advanced metering in flanders (belgium). In *IEEE Instrumentation and Measurement Technology Conference Proceedings.*, 2008.

[7] D. M. F. Baker. Internet protocols for the smart grid. Rfc 6272, Cisco Systems, 2011.

[8] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid - the new and improved power grid: A Survey. *IEEE Communications Surveys & Tutorials*, 14(4):944–980, 2012.

[9] H. Farhangi. The path of the smart grid. *IEEE Power and Energy Magazine*, 8(1):18–28, 2010.

[10] H. Gharavi and B. Hu. Multigate communication network for smart grid. *Proceedings of the IEEE*, 99(6):1028–1045, 2011.

[11] V. Gungor and F. Lambert. A survey on communication networks for electric system automation. *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 50(7):877–897, 2006.

[12] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke. Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, 7(4):529–539, Nov 2011.

[13] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke. A survey on smart grid potential applications and communication requirements. *IEEE Transactions on Industrial Informatics*, 9(1):28–42, Feb 2013.

[14] J. Kim, D. Kim, K. Lim, Y. Ko, and S. Lee. Improving the reliability of IEEE 802.11s based wireless mesh networks for smart grid systems. *Journal of Communications and Networks*, 14(6):629–639, Dec 2012.

[15] B. Lichtensteiger, B. Bjelajac, C. Muller, and C. Wietfeld. RF Mesh systems for smart metering: System architecture and performance. In *IEEE International Conference on Smart Grid Communications*, 2010.

[16] J. Liu, B. Zhao, J. Wang, Y. Zhu, and J. Hu. Application of power line communication in smart power consumption. In *IEEE International Symposium on Power Line Communications and Its Applications*, 2010.

[17] W. Luan, D. Sharp, and S. Lancashire. Smart grid communication network capacity planning for power utilities. In *IEEE PES Transmission and Distribution Conference and Exposition*, April 2010.

[18] R. Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar. A survey on advanced metering infrastructure and its application in smart grids. In *Proceedings of the 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–8, Toronto, ON, CAN, 2014. IEEE.

[19] K. Moslehi and R. Kumar. A reliability perspective of the smart grid. *IEEE Transactions on Smart Grid*, 1(1), 2010.

[20] NIST. NISTIR 7761 - Guidelines for assessing wireless standards for smart grid applications, 2011.

[21] NS-2. The network simulator - ns-2, 2013.

[22] P. Parikh, M. Kanabar, and T. Sidhu. Opportunities and challenges of wireless communication technologies for smart grid applications. In *IEEE Power and Energy Society General Meeting*, 2010.

[23] D. Passos and C. Albuquerque. A joint approach to routing metrics and rate adaptation in wireless mesh networks. *IEEE/ACM Transactions on Networking*, 20(4):999–1009, Aug 2012.

[24] N. Saputro, K. Akkaya, and S. Uludag. A survey of routing protocols for smart grid communications. *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 56(11):2742 – 2771, 2012.