Denial of Service Attacks and Mitigation for Stability in Cyber-Enabled Power Grid

Pirathayini Srikantha and Deepa Kundur
The Edward S. Rogers Sr. Department of Electrical and Computer Engineering
University of Toronto
Email: {pirathayini.srikantha, dkundur}@ece.utoronto.ca

***Abstract*—Monitoring and actuation represent critical tasks for electric power utilities to maintain system stability and reliability. As such, the utility is highly dependent on a low latency communication infrastructure for receiving and transmitting measurement and control data to make accurate decisions. This dependency, however, can be exploited by an adversary to disrupt the integrity of the grid. We demonstrate that Denial of Service (DoS) attacks, even if perpetrated on a subset of cyber communication nodes, has the potential to succeed in disrupting the overall grid. One countermeasure to DoS attacks is enabling cyber elements to distributively reconfigure the system's routing topology so that malicious nodes are isolated. We propose a collaborative reputation-based topology configuration scheme and through game theoretic principles we prove that a low-latency Nash Equilibrium routing topology always exists for the system. Numerical results indicate that during an attack on a subset of cyber nodes, the proposed algorithm effectively enables the remaining nodes to converge quickly to an equilibrium topology and maintain dynamical stability in the specific instance of an islanded microgrid system.**

I. Introduction

Today's power grid is an extremely complex entity composed of many interconnected tightly coupled components. In order to ensure that the power grid is functioning well, monitoring devices such as the Phasor Measurement Units (PMU) are being extensively deployed at many points of the grid [6]. PMUs take local magnitude and phase information of associated voltages and currents, amongst other quantities, and transmit this information to a centralized Data Concentrator (DC) at a frequency ranging from to 50 to 60 Hz [4]. This data can be used to make critical control decisions to maintain the stability of the grid. For example, microgrids functioning in islanded mode represent subsystems that must rely heavily on real-time measurement and control for maintaining a balance between variable generation and demand.

In order to present a real-time snapshot of the grid, measurements reported by the PMUs must be transmitted over a communication route with good quality of service (QoS) factors such as low latency and data loss. Although the PMU communication infrastructure is still largely under development, one possible configuration includes employing short-range wireless relay nodes (RNs) which form a multi-hop network for data transmission. PMUs and their associated RNs are susceptible to cyber-physical security vulnerabilities and therefore are prone to cyber attacks such as Denial of Service (DoS). DoS attacks that compromise RNs can manipulate these to behave in the following manner: drop all forwarded packets, inject false routing information to partition the network, flood false data to consume system resources, selfishly access medium and many more [2]. These malicious actions will significantly impact the QoS of data traversing through the network possibly rendering the associated information no longer relevant.

DoS attacks perpetrated on the cyber network of the power grid are similar to those identified in ad-hoc wireless networks. Many classical schemes have been proposed in the existing ad-hoc routing literature that circumvent these security issues via distributive topology formation techniques that enable cooperation between well-behaved RNs by rewarding these with virtual currencies [2] or reputation [3]. In this work, a reputation-based distributed topology formation algorithm has been proposed which differs from existing protocols as it is tailored specifically to reduce overall routing latency in the system caused by misbehaving RNs. We also use game theoretic principles to prove that well-behaved unpartitioned RNs will always converge to a low-latency Nash Equilibrium topology via myopic local link formation decisions. We show that without this algorithm, delays introduced by attacks render the system unstable while when this algorithm is active, dynamical stability is maintained.

In the existing literature, as per the authors' knowledge, the impact of DoS cyber attacks combined with the demonstration of the existence of an effective countermeasure in the context of physical stability in the power system has not yet been explored. In [12], Ustun *et al.* present a communication protocol that can be used by cyber elements to form a network topology for routing in a microgrid based on the Dijkstra's algorithm. Security or QoS factors are not taken into consideration in this proposal. The impact of the proposed routing mechanism on the dynamics of the microgrid is not demonstrated either. In [8], Macana *et al.* explore the impact of communication latency on the dynamics of a microgrid. However, a specific algorithm is not proposed to overcome communication latency. In [7], the authors demonstrate the impact of DoS attacks on load frequency control of the grid but do not propose any countermeasures.

The remainder of this paper is organized as follows. Section II details the assumptions and threat model used in this work. Section III presents the formulation of the distributed topology formation algorithm along with a game theoretic analysis. Section IV contains results on the convergent characteristics,

978-1-4799-1785-3/15/$31.00 ©2015 IEEE

network topology and stability when the cyber network of an islanded microgrid is subjected to attack with and without the integration of the proposed algorithm. Finally, in Section V, possible future directions and concluding remarks are made.

II. System Model

Notations and assumptions used in the formulation of the threat model and proposed countermeasure are presented in this section.

A. Cyber Network

The network topology containing the RNs that form the cyber network overlay with the power system is represented by an undirected graph $G(V, E)$ which defines a set of paths in E that can be used by RNs in $V = \{r_1 ... r_{n+1}\}$ for routing data. RNs can function as PMUs, cyber-actuators, relays and/or an Agent. PMUs generate measurement data and cyber-actuators make changes to physical components in the system based on cyber signals. Relays function as intermediaries aiding with the transmission of data. Agent functions as a sink receiving PMU data or as a source transmitting control signals to cyber-actuators. E defines all active paths in the topology as a set of pairs (r_i, r_j) where $r_i, r_j \in V$. In this work, each node utilizes local information to select its parent node, thereby enabling the distributive formation of a connected network topology. Two link formation constraints are imposed on the nodes. Firstly, r_i is restricted to choosing its parent only from the set S_i which contains the 'neighbouring' nodes of r_i. Nodes can be neighbours of r_i based on spatial constraints (e.g. transmission range). Secondly, r_i is restricted in the maximum number of connections D_i it can accept from other nodes so that a balance in the routing workload throughout the network is maintained.

The network topology is hierarchical and has a tree-like structure. The Agent is at the root. It broadcasts control data to its descendants until the data reaches the leaf nodes in the network topology. PMUs propagate measurement data to parent nodes which in turn will do the same until data reaches the Agent node. Figure 1 illustrates an example of all possible connections in a simple network topology used for an islanded micro grid system.

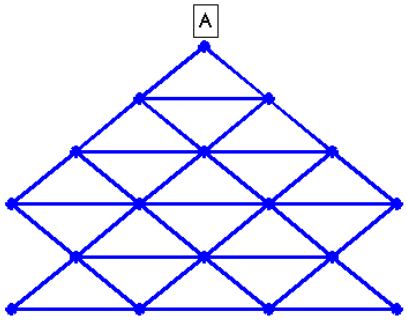

Fig. 1. Network Topology containing 16 RNs and an Agent. Graph showing all allowed connections.

B. Threat Model and Assumptions

In our threat model, we make the following assumptions:

1) DoS attacks will compromise one or more RNs to either selfishly use the available medium or drop all forwarded packets.
2) PMUs are deployed in redundantly in the grid.
3) Attacked nodes do not partition the Agent from the unaffected nodes.
4) Each RN can securely encrypt embed routing information such as bandwidth and hop count into data or control packets.
5) RNs will request for routing information from its neighbouring RNs.
6) Only one Agent exists in the topology.

The first assumption ensures that the DoS attacks are internal. These attacks are more subtle and harder to detect than external attacks such as jamming [2]. Second assumption ensures that there is sufficient redundancy in PMU deployment so that the Electric Power Utility can still make an accurate state estimation even when a small set of PMUs is compromised. The third assumption ensures that no subset of un-compromised RNs can be isolated from the Agent due to partitioning. The fourth assumption ensures that information about the characteristics of a routing path is always accurate can be implemented with tamper-proof hardware installed in RNs [3]. The fifth assumption ensures that RNs can communicate locally to enable collaborative network formation. If an RN does not respond to the request, the requesting RN will assume that it is compromised. The final assumption implies that there exists only one data concentrator for a network of RNs.

III. Distributed Topology Formation Algorithm

In this section, a detailed overview of the proposed distributed topology formation algorithm is presented.

A. Cost Function

Each RN r_i is associated with a cost J_i that represents the "reputation" of that node. Higher this value is, the lower is the reputation of the corresponding RN. An RN will choose one of its neighbours as a parent link based on this reputation/cost factor. Hence, the cost should be constructed to penalize undesirable features and reward desirable characteristics of RNs composing the path to Agent A. We define the cost function associated with r_i to be:

$$J_i = H_A^{r_i} + 1 + \underset{s_j \in P_{r_i}}{max} \ (e - q^{s_j})^2 \tag{1}$$

where $H_A^{r_i}$ is the hop count from r_i to A, P_i is the set of RNs forming the path from r_i to A, e is the expected bandwidth of an RN and q^{s_j} is the bandwidth of RN s_j located on the path between r_i and A. The first term in Equation 1 penalizes r_i for choosing a parent s_i whose path to A has too many hops; if s_i has no path to agent A, then $H_A^{r_i}$ is set to a very high number to penalize the node for not being connected to A. When the second term $>> 0$, this implies that one RN on the path to A is behaving in an abnormal manner as it is either not forwarding any packets or transmitting too many packets.

Distributed Topology Formation Algorithm by r_i

1) Compute τ using exponential distribution with $\lambda = 2$sec.
2) After τ seconds, request $q_{max}^{s_i}$ and $H_A^{s_i}$ from every $s_i \in S_i$.
3) Compute J_i based on this information for all $s_i \in S_i$.
4) If $s_i = \underset{s_i \in S_i}{\text{argmin}}\ J_i$ then set parent to be s_i.
5) Send updated $q_{max}^{s_i}$ and $H_A^{s_i}$ information to descendants.
6) Descendants will update individual costs according to Steps 2,3.

TABLE I
DISTRIBUTED SECURE ROUTING ALGORITHM

B. Distributive Implementation

Every r_i can compute its reputation based on its local properties such as bandwidth and choice of parent node in a distributive manner. The total hop count from r_i to A if s_i is its parent is the number of hops required for s_i to reach A incremented by one. It is not necessary for r_i to have bandwidth information of every RN on its path to A to compute the second term of J_i. r_i can evaluate this by simply using it own bandwidth information and the maximum bandwidth information of its parent s_i according to $\max\{(e - q^{r_i})^2, \max_{s_j \in P_{s_i}}(e - q^{s_j})^2\}$. Hence, r_i can compute its reputation simply based on its local and its parent's properties. If r_i does not receive any information from a particular neighbour, it will not consider it in the parent selection process. The RN that the node r_i will select is the neighbour that is most reputable (i.e. results in the least cost) and this is in essence a myopic selection approach. The parent chosen by r_i will affect only the cost functions of its descendants. If r_i changes its parent, then it will transmit its updated $max_{s_j \in P_{r_i}}\ (e - q^{s_j})^2$ and hop count information to its descendants. Descendants will similarly update their costs. This will continue until the cost information propagates to the leaf nodes of the network topology. All RNs will individually set a random timer that is exponentially distributed with a mean of 2 seconds. This is the average communication latency expected in the system. An RN re-evaluates its current parent node selection when its timer expires according to the complete algorithm is listed in Table I.

C. Game Theoretic Analysis

Next, we show that the proposed distributed topology formation algorithm has interesting equilibrium properties through game theoretic analysis. When the proposed algorithm is in effect, all nodes essentially participate in an n player game to distributively determine a secure network topology. This game is denoted by $\mathcal{G}(I, S_i, J_i)$ where I is the set containing all n players, S_i contains all the possible actions available to player r_i and J_i is the cost function assigned to player r_i [10]. As Agent A does not need to select a parent, it will not participate in the game. Hence, players in I consist of nodes in $V \setminus A$. An action taken by r_i involves selecting a parent node from its neighbours. For this reason, S_i consists of all the neighbours of r_i. s_i is the parent node selected by r_i and s_{-i} are the parent nodes selected by all other players (i.e. $I \setminus r_i$). $J_i(s_i, s_{-i})$ is the cost function of player r_i which is dependent on the actions of all other players in the system. Each player is assumed to be rational but selfish. In other words, each player will attempt to minimize its own cost regardless of what happens to others. Best-response strategy is one approach nodes can take in which r_i selects a strategy from the best response correspondence set $\Phi_i(s_i)$ defined in Equation 2. The set $\Phi_i(s_{-i})$ contains all strategies that r_i can take that will result in the least cost for it given that all other nodes have selected strategy s_{-i}.

$$\Phi_i(s_{-i}) = \{s_i^* | J_i(s_i^*, s_{-i}) \leq J_i(s_i, s_{-i}); \forall s_i \in S_i\} \quad (2)$$

Many types of equilibria can be reached by nodes playing the game $\mathcal{G}$ using the best response approach. In this work, Nash equilibrium (NE) is considered. At NE, players will have no regret in choosing their respective strategies. More specifically in the context of this work, when NE is attained, a node participating in the topology formation game cannot choose as parent another node without incurring more cost. This can be formally stated as:

$$J_i(s_i^*, s_{-i}^*) \leq J_i(s_i, s_{-i}^*); \forall s_i \in S_i, \forall i \in I \quad (3)$$

where s_i^* and s_{-i}^* are the strategies that result in NE. When the game has reached this point, there is no incentive for any node to deviate from its current strategy as this can result in a higher cost for that node.

In order to determine the existence of an NE for this game formulation, the notion of potential games is employed. If it is possible to define a global function V^G for the topology G that satisfies the condition in Equation 4, then the game can be classified as an ordinal potential game (OPG) which is a class of network formation games [11].

$$\begin{aligned} V^G(t_i, s_{-i}) - V^G(s_i, s_{-i}) > 0 \iff \\ J_i(t_i, s_{-i}) - J_i(s_i, s_{-i}) > 0 \\ \forall i \in I, \forall t_i \in S_i, \forall s_i \in S_i, \forall s_{-i} \in S_{-i} \end{aligned} \quad (4)$$

If such a potential function can be defined, then it can be said that an NE exists for the game [9]. It is shown next that a V^G satisfying this condition exists for $\mathcal{G}$.

D. Potential Function

Consider the potential function based on the cost function J defined as follows:

$$V(s_i, s_{-i}) = \sum_{j=1}^{n} J_j(s_i, s_{-i}) \quad (5)$$

The cost incurred by player r_i is directly affected by the cost incurred by its parent. Suppose, that the cost of using strategy s_i is lower than that of using strategy t_i for

node r_i (i.e. $J_i(s_i, s_{-i}) < J_i(t_i, s_{-i})$). This implies that either the bandwidth is closer to the expected value (i.e. $max_{s_j \in P_{s_i}} (e - q^{s_j})^2 < max_{s_k \in P_{t_i}} (e - q^{s_k})^2$) or hop count to A has decreased (i.e. $H_A^{s_i} < H_A^{t_i}$). If the only node changing its strategy from t_i to s_i is node r_i and all other nodes do not change their strategies, the nodes that are parents of r_i will be unaffected as r_i is not on their path to A. Nodes that will be affected by this switch are the descendants of r_i. The cost functions of the descendants will also decrease or remain the same as either the bandwidth level is closer to the expected value or the overall hop count for a portion of the path of r_i's descendants to A has decreased. Therefore,

$$\begin{aligned} J_j(s_i, s_{-i}) &= J_j(t_i, s_{-i}); \text{ if } j \in P_i \\ J_j(s_i, s_{-i}) &\leq J_j(t_i, s_{-i}) \text{ if } j \in C_i \end{aligned} \tag{6}$$

where P_i are the parent nodes of r_i and C_i are descendent nodes of r_i. From this, the following deductions can be made.

$$\begin{aligned} &V(t_i, s_{-i}) - V(s_i, s_{-i}) = \\ &\sum_{j=1}^{n} J_j(t_i, s_{-i}) - \sum_{j=1}^{n} J_j(s_i, s_{-i}) = \\ &J_i(t_i, s_{-i}) - J_i(s_i, s_{-i}) + \\ &\sum_{j \in C_i} [J_j(t_i, s_{-i}) - J_j(s_i, s_{-i})] > 0 \\ &\iff J_i(t_i, s_{-i}) - J_i(s_i, s_{-i}) > 0 \end{aligned} \tag{7}$$

Hence, since an ordinal potential function has been identified, it can be concluded that an NE always exists for this game.

IV. Modelling and Results

In this section, numerical results illustrating the impact on the physical stability of an islanded microgrid system with and without the deployment of the proposed algorithm when a DoS attack is perpetrated on a subset of RNs in the cyber network are presented. We also numerically show that the theoretical result obtained in the previous section indicating the existence of a NE routing topology holds for the specific system considered here.

A. Cyber-Physical Modelling

First, the dependencies between cyber and physical entities are established for the power system under consideration. The physical system is an islanded microgrid illustrated in Figure 2 (used for example in [8]) that relies on measurement information obtained at high frequency regarding the load and the power dispatched by distributed generation sources in order to effectively control the system. This measurement data is communicated to a central controller via physical nodes composed of PMUs or RNs that form the cyber network. The central controller assimilates this data and computes actuation signals that are transmitted to cyber-actuators through the same node network.

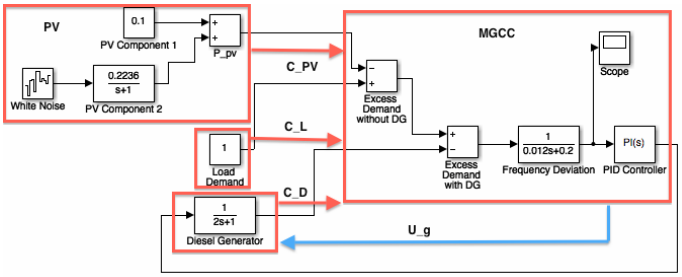

Fig. 2. Control block of islanded microgrid

1) Cyber Network: The network illustrated in Figure 1 is the spatial configuration of PMUs and nodes considered in this paper. Solid lines represent allowed connections or edges between RNs. When two RNs have an edge between each other, each will be a member of the other RN's neighbourhood set S_i. The maximum allowable children for any RN is assumed to be 3 (i.e. $D_i = 4$). Any of these RNs except for the Agent can be subjected to a DoS attack. The attack will attempt to increase or drop packets forwarded by the attacked r_i.

2) Islanded Microgrid: The cyber network in Figure 1 is implemented as an overlay of the islanded microgrid system illustrated in Figure 2. The architecture, control structure and parameters for the implementation of the microgrid system are adapted from [8]. The system is composed of a photovoltaic (PV) generator, a diesel generator (DG), a constant demand source and a microgrid central controller (MGCC). The red arrows in the control block represents the transmission of measurement data which is fed into the PID controller of the MGCC to send control signals to the DG to regulate the dynamic stability of the system.

B. Results

The network and the islanded microgrid system are implemented in MATLAB using parameters in [8]. When RNs are functioning regularly, the routing topology obtained via the proposed routing algorithm is expected to be a regular tree-like structure. Suppose that two RNs marked in red in Figure 3 are subjected to DoS attacks. Any traffic traversing these nodes will be subjected to extreme delays.

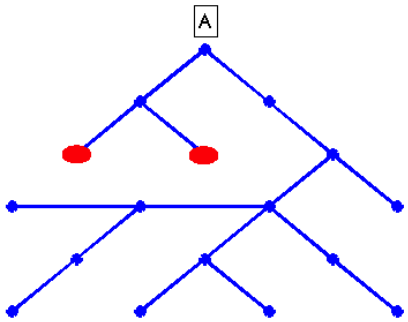

Fig. 3. Topology formed with the proposed algorithm

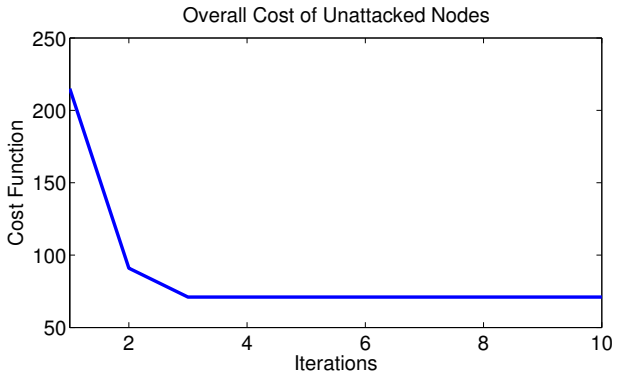

Fig. 4. Aggregate cost incurred by well-behaving nodes

The routing algorithm must enable cyber nodes to form a new topology in a distributed manner so that the attacked RNs are circumvented. Figure 3 illustrates the final network topology when the proposed algorithm is applied. This shows that the algorithm allows nodes to successfully converge to the desired topology in a distributed manner during the advent of an attack on multiple RNs in the system. The algorithm is executed for 10 iterations and the total costs obtained for all un-attacked nodes in the system for each iteration is illustrated in Figure 4. It is evident that the cost of each node is decreasing at every iteration until the topology converges to NE, at which point the overall cost in the system does not change. Since the network is relatively small, convergence to equilibrium is achieved quickly in 3 iterations. It has been numerically verified that fast convergence also holds for larger cyber networks. These results reinforce the game theoretic result obtained earlier which states that an NE is guaranteed to exist to which the network topology will converge to.

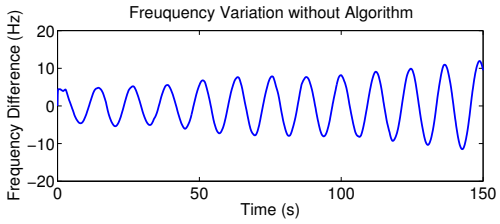

Fig. 5. Without Algorithm

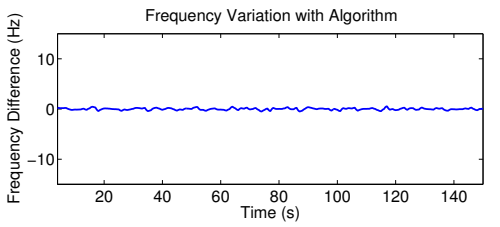

Fig. 6. With Algorithm

Suppose that the topology of the network is fixed permanently and no dynamic topology algorithm is used by the nodes to intelligently forward data. The impact of this attack on the stability of the islanded microgrid is illustrated in Figure 5. It is clear that the delay in the measurement data results in the system veering off into instability. This clearly illustrates the importance of maintaining low latency in the network.

In contrast, when the proposed routing algorithm is applied to the network and the two RNs are subject to attack, the resulting frequency deviation in the islanded microgrid is illustrated in Figure 6. It is clear that even when the network is subject to attacks, the cyber nodes have reconfigured themselves so that the resulting frequency deviation is maintained close to 0. Hence, the islanded microgrid remains stable even when the system is under attack. This illustrates the strength of the proposed algorithm.

V. Conclusions

In this work, we have demonstrated that DoS attacks can significantly affect the physical stability of a power system like the islanded microgrid and countermeasures such as the proposed distributed topology formation algorithm exist to circumvent the impact of these. We have demonstrated the ability of this algorithm to successfully isolate attacked cyber nodes so that data can continue to be transmitted at low latency. It is shown that the cyber nodes are able to converge to an NE topology while taking into account security and QoS considerations. As future work, the impact of DoS attacks on other types of power systems with significant inertia like the main grid should be investigated.

References

[1] Ivo Adan and Jacques Resing. Queueing theory. *Course Notes Eindhoven University of Technology*, pages 1 – 180, 2002.

[2] Jamal N. Al-Karaki and Ahmed E. Kamal. Stimulating node cooperation in mobile ad hoc networks. *Journal Wireless Personal Communications*, 44(2):219 – 239, 2008.

[3] Sonja Buchegger and Jean-Yves Le Boudec. Performance analysis of the confidant protocol. *ACM international symposium on Mobile ad hoc networking and computing*, pages 226 – 236, 2002.

[4] Young Jin Kim, M. Thottan, V. Kolesnikov, and Wonsuck Lee. A secure decentralized data-centric information infrastructure for smart grid. *IEEE Communications Magazine*, 48(11):58–65, 2010.

[5] B. Santosh Kumar and S. Mishra. Agc for distributed generation. *ICSET*, 2008.

[6] Deepa Kundur. Security seminar. *Course Notes University of Toronto*, 2013.

[7] Shichao Liu, Xiaoping P. Liu, and Abdulmotaleb El Saddik. Denial-of-service (dos) attacks on load frequency control in smart grids. *IEEE PES Innovative Smart Grid Technologies (ISGT)*, pages 1 – 6, 2013.

[8] Carlos Andres Macana, Eduardo Mojica-Nava, and Nicanor Quijano. Time-delay effect on load frequency control for microgrids. *IEEE International Conference on Networking, Sensing and Control*, pages 544 – 549, 2003.

[9] Dov Monderer and Lloyd S. Shapley. Potential games. *Journal of Economic Literature*, 14(44):124143, 1996.

[10] Lacra Pavel. Game theory and evolutionary games. *Course Notes University of Toronto*, 2013.

[11] Eva Tardos and Tom Wexler. Network formation games and potential function method. *Course Notes Cornell University*, 2007.

[12] Taha Selim Ustun, Cagil Ozansoy, and Aladin Zayegh. Implementation of dijkstras algorithm in a dynamic microgrid for relay hierarchy detection. *IEEE International Conference on Smart Grid Communications*, pages 481 – 486, 2011.