Using Self-Organizing Architectures to Mitigate the Impacts of Denial-of-Service Attacks on Voltage Control Schemes

Calum Cameron, Charalampos Patsios, Phil C. Taylor, *Senior Member, IEEE*, and Zoya Pourmirza, *Member, IEEE*

***Abstract*—Modern power systems are becoming increasingly decentralized, with a greater degree of observability provided through a network of sensors and local controllers in addition to existing centralized supervisory control and data acquisition platforms. However, the interconnectivity between sensors and controllers creates potential vulnerabilities which can be exploited by a cyber-attack. The majority of components installed on the grid were designed with little or no consideration for aspects of cyber-security and therefore leaving the network at risk of economic loss, asset damage or widespread blackouts. Present research in cyber-attack events and electrical grid resilience, often treats these in isolation. Furthermore, the ICT infrastructure in modern electrical networks is not tested as rigorously in terms of reliability and security as the physical assets. Therefore, an integrated approach is needed for the analysis of cyber-threats against power systems, linking the attack mechanisms in the ICT layer and the physical impacts at the electrical layer. This paper introduces a method of self-organizing communication architectures that for the first time has been applied to the problem of mitigating the negative impacts of denial of service cyber-attacks in the smart grid and demonstrates the benefits of this in a novel integrated environment connecting power system modeling and communication layer simulation. This paper demonstrates and quantifies the advantages of self-organization in terms of computational burden and voltage control in a distribution network experiencing multiple attack formats and increasing numbers of attackers.**

***Index Terms*—Smart grid, self-organizing systems, multi-agent systems, cyber-security, voltage control.**

I. Introduction

IT IS widely accepted that modern energy networks are gravitating towards greater integration of smarter technologies. These technologies are intended to deliver increased observability and distributed control for the purposes of implementing more advanced smarter grids. This evolution is driven by numerous factors including distributed generation, energy storage and demand side response. Such advancements rely on a sophisticated Information and Communication technology (ICT) which bring more intelligence into the grid by tranceiving sensor measurements and control signals. However, this reliance on interconnected systems creates vulnerabilities which can be exploited through cyber-attacks. Additionally, cyber-interdependency of the smart grid creates vulnerabilities for the electrical grid. Smart Grid cyber interdependency exists because the state of the physical infrastructure depends on the information transmitted through the ICT infrastructure [1]. In the United States 170 electrical outages have been triggered by cyber-related causes [2]. Due to minimal post-event, digital forensics specific information on the set of attack strategies used is not available, but this demonstrates that damaging the ICT infrastructure can trigger physical power outages. Vulnerabilities in the ICT layer can also be triggered by hardware failures or through malicious intent in a targeted cyber-attack [3], [4]. The risk of cyber-attack is also a consequence of legacy systems in operation within the electrical grid. Several Supervisory Control and Data Acquisition (SCADA) systems were initially developed without cyber-security considerations [5], these intelligent monitoring systems provides the communication infrastructure across the electrical grid from 11 kV to 132 kV. Even present ICT systems lack the strenuous testing regimes applied to physical network assets [6].

Present research indicates that the methods of modeling cyber-attacks and those evaluating power system vulnerabilities are considered separately, not in an integrated manner [7]. Additionally, research into cyber-security fail to sufficiently model the physical power system. Instead focusing on smart-grid measurement data and communication protocols [8]. Firstly, this limits the degree which the impacts of a cyber-attack can be assessed and quantified, subsequently leading to inaccurate or inconclusive assessments of the value and prioritization of defense mechanisms. Secondly as an attack event can vary in scale, duration and format is it important that the physical system – i.e., the electrical network is studied as the attack develops.

Consequently, this calls for integrated cyber-physical modeling approaches. Vellaithurai *et al.* [9] explicitly state that a combined cyber-physical analysis is required to establish the impacts of a cyber-attack event on the physical system. Such analysis methods can enable the development

Manuscript received January 16, 2017; revised June 15, 2017 and January 12, 2018; accepted March 8, 2018. Date of publication April 3, 2018; date of current version April 19, 2019. This work was supported by the Engineering and Physical Science Research Council, U.K., as part of the grand challenges project "The Autonomic Power System." Paper no. TSG-00082-2017. *(Corresponding author: Calum Cameron.)*

The authors are with the School of Electrical and Electronic Engineering, Newcastle University, Newcastle upon Tyne NE1 7RU, U.K. (e-mail: calum.d.cameron@outlook.com; p.c.taylor@newcastle.ac.uk; haris.patsios@newcastle.ac.uk; zoya.pourmirza@newcastle.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2018.2817046

of methods to mitigate the physical impacts based on procedures carried out in the cyber-layer. Methods which are complimentary to other defensive mechanisms such as physical security, data validation and encryption. Reconfiguration through self-organization has been demonstrated in several research domains for a variety of problems such as underwater sensor networks [10] and wireless communications [11] and traffic management [12]. Self-organization has also been applied with respect to power-system applications as presented by Zhang *et al.* [13] and Lin *et al.* [14]. However, these examples do not take account the influence of an attack in the form of a Denial of Service (DoS). Cohen [15] indicate that few defensive mechanisms exist to counter a DoS attack within the context of a smart-grid environment.

The work presented in this paper illustrates the value of a novel implementation of a self-organizing architecture through an integrated modeling approach to mitigate the impacts of a series of DoS attacks. Where the attack objective is to compromise voltage control availability within a multi-agent smart-grid distribution network. Previously indicated work [13] and [14] does not consider attack mitigation in the presence of an active control problem and where components responsible for delivering control are under attack. Attack detection, recovery, and self-organizing communication routing are important factors in maintaining system operation. Maintaining controllability remains equally as imperative and has a measurable impact on the physical components under the jurisdiction of the IT network.

Section II of this paper discusses the general cyber-security concerns of the smart-grid, threats posed by them, and how would they affect the grid. Also, this section discusses the importance of a DoS attack. Section III outlines the supporting research and the implementation of the SOA. Section IV documents the approach to evaluating the SOA, including the problem scenario, attack modeling and integrated test platform involved. Section V illustrates the results of comparing the SOA with a typical static smart grid architecture. Finally, Section VI offers conclusions and avenues for further work.

II. Importance of the Problem Domain

Currently, the power grid suffers from lack of technical or operational solutions to prevent or withstand cyber-attacks [16]. Utilities could benefit from investigating and identifying a number of cyber-security goals and their respective attack scenarios, using modeling techniques to understand the effects of an attack, and the ability of the grid to withstand them.

National Institute of Standards and Technology (NIST) has defined three cyber-security goals for Smart Grids, which are availability, integrity, and confidentiality. Although data confidentiality has the highest importance for any IT system it is not an immediate threat to the power grid. Availability, followed by integrity in terms of prioritization is more critical for Smart Grids.

A confidentiality attack refers to an attack which aims to gain unauthorized access to sensitive customer or measurement data, an example attack vector being social engineering. Such an attack strategy would not necessarily have a physical impact on the electrical grid, but can be a preparatory step to a more damaging attack. It could be used to steal access credentials or rights from operators. For example, a social engineering mechanism called spear-phishing was employed in cyber-attack on Ukrainian power grid [17]. This was used to steal access credentials to the system to facilitate easier installation of remote access tools, handing control of the system over to the adversary. Counteracting this attack is difficult from a technical point of view, as it targets a human controller, rather than a machine controller.

An Integrity attack refers to confirming that information in transit between various elements of the grid are trusted, accurate, and have not been manipulated or fabricated. A false data injection is one of the attack vectors that could compromise integrity of the Smart Grid [18]–[21]. This data tampering can take place in many formats, from misrepresenting sensor data to trick state estimation systems [22] or falsify network topologies [23]. Data tampering attacks can trigger controllers to make incorrect decisions resulting in economic losses and operational issues [24]. Researchers have investigated the vulnerability of state estimation under data tampering attack, such that false data is accepted by the estimator bypassing bad data filtration processes [22], [24], and [25]. Although these systems contain contingency techniques such as filtering and/or removing bad data, the attackers continually develop new methodologies to evade error detection solutions to inject false data into state estimators. This attack would affect the grid by reducing the awareness of component failure and leading to incorrect decision-making. Another data tampering attack strategy involves misleading the control center by forging network topology information [23]. This attack vector exploits the lack of authentication between terminals and the control center, thus convincing the control center that the network is operating under a different topology. False data injection for forging network topology would affect the grid by concealing the network stress and preventing control actions being initiated to relieve those stresses.

Availability refers to confirming that information is available in a timely manner. Accordingly, this paper focuses on this cyber security goal. In conventional grids, utilities estimate meter readings with limited information. Thus unavailability of meter data was of little threat to the system. However, in a smart grid context, smart meter readings with sensitive information and control signals are being exchanged between several entities. Therefore, availability, especially in the case of delivering control signals is crucial within the smart grid.

The importance of availability in the smart grid are most evident in networks where Advanced Metering Infrastructure (AMI) is implemented, and where traffic loads can compromise the availability of the overall system. In a system where the AMI is responsible for transmitting outage alarms and managing distributed generation, distribution automation or other critical functions, it is important to facilitate the timely movement of data, even when the network is flooded with data or under attack [26].

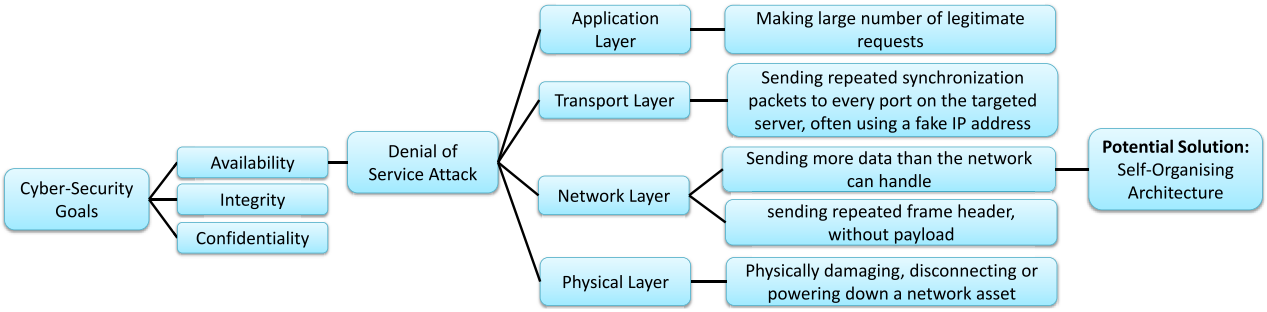

Fig. 1. Attack Description.

Additionally, data availability can affect all layers of Internet protocol stack (called TCP/IP), which also defines the importance of data availability as a high priority requirement of a smart grid communication network. For example, availability can be affected by device tampering in the physical layer of the protocol stack, by traffic manipulation in data link layer, by false routing in network layer, and by flooding in transport layer. Data availability and integrity can be compromised through several means: worms, viruses, malware, phishing, and denial of service (DoS) attacks. DoS can be carried out by data flooding the nodes or resources in a network to prevent genuine requests from being processed. In this paper we investigate DoS because this attack can be applied to all the layers of the TCP/IP protocol stack, therefore making it an important threat to the system. Additionally, there has been growing reports of a DoS attack format being used against power systems. The two most notable cyber-attacks reported in recent years are Stuxnet [27] and Ukrainian [17] events, where in both cases attackers used a DoS attack strategy to disturb the power grid. Other research such as presented in [28] also supports the assumption that DoS is amongst the most dangerous security threats to the smart grid.

The impacts of such DoS attacks on the power system have significant consequences for performing control and potentially lead to physical component damage, financial losses and outages, triggered by control signal loss. This paper discusses the DoS attack modeling in detail and examines a number of different DoS attack scenarios, in the form of Burst, Sequential and Continuous Low Rate DoS formats. Additionally, each format follows both an Adaptive and a Static attack approach. To illustrate the contribution of this research Fig. 1, is presented, documenting the global view of cyber attacks in order of priority, focusing on availability. Due to the widespread influence of data availability, all layers of the TCP/IP stack can be influenced by a DoS event as depicted in Fig. 1. For example as DoS attacks can affect the application layer through producing a large number of seemingly legitimate data. The transport layer is vulnerable to IP spoofing and excessive transmission of synchronization packets. The network layer can be influenced by large volumes of traffic which can delay control responses. Finally, the physical layer can be affected by a DoS attack through physically damaging, disconnecting or powering down a network asset. It is believed [15] that the cyber-physical network has few options in defensive approaches in the face of a denial of service attack other than purchasing additional bandwidth.

This paper describes a novel integrated environment which implements and evaluates a self-organizing multi-agent architecture through cyber-physical simulation. Previous work by the authors presented in [29], supported by literature indicates the applicability of self-organizing approaches in relation to providing adaptability to smart-grid systems. The previous work evaluated a set of static architectural configurations in relation to performance objectives including data congestion, voltage control performance and communication response times.

These examinations demonstrated that across differing agent population sizes and topologies no single configuration delivered optimum performance. Therefore, demonstrating the need for greater flexibility in the form of self-organization. This work serves as an extension to the previous publication whereby the implemented architecture is applied as a defensive mechanism with respect to mitigating the impacts of a Denial of Service (DoS) attack.

III. A Self-Organizing Architecture

The previous research indicated the potential value of a SOA, however the work presented in this paper examines the feasibility of developing such an architecture. Furthermore the work provides additional contributions in demonstrating the SOA with continuous performance monitoring, decision-making and an initial configuration stage. The SOA is then demonstrated with respect to a cyber-security threat illustrating value in addition to that suggested in previous work, within an integrated test platform.

A. Current Architectures

Given the wide research interest in smart grid implementations there are a range of control and communication architectures in use. As illustrated in [30]–[32] smart grid IT architecture deployments are predominantly hierarchical in nature which in turn correlates to the structure of the power system under observation. Furthermore, there is a trend in applying local control to smaller sub-sections of the monitored network as documented in [33]–[35]. This local control approach increases decentralization and removes the threat presented by a single point of failure. Architectures presented

in literature display a trend for three core component tiers. The lowest tier contains customer level entities, typically in the form of smart meters, and distributed generation. The intermediary layer is composed of local controllers and data collection components, while the highest tier contains a central server for processing global data and control objectives.

B. Self-Organization

A self-organizing system can be defined as one that can satisfy the requirements of: scalability, robustness, flexibility and adaptability [36]. Research by Serugendo *et al.* [37] add further properties including the ability to form structures automatically, and the ability to perform self-monitoring. SOAs have been applied to multiple research sectors, and in each case the drivers for restructuring and reconfiguration mechanisms are tailored to the problem domain. This demonstrates the universality of a self-organizing solution and therefore its applicability to a smart grid scenario. Some systems apply self-organization in terms of agent roles and behaviors, while others apply mechanisms for the restructuring of connections within the architecture. Given the universality of self-organizing systems, they have numerous applications within the smart grid research domain – Srivastava *et al.* [38] implement self-organization to increase network resilience in the event of agent failure through passing roles to agents in a different hierarchical tier.

In addition to accounting for physical entity failure the smart grid research community has applied self-organization for further elements of network resilience in the form of mitigation against cyber-threats as presented by Lin *et al.* [14]. The work describes a self-healing mechanism surrounding phasor measurement units, whereby is a node becomes compromised by an attack it is disconnected. After an attack data and communication is re-routed via surviving nodes to maintain observability. This work differs from the proposed methodology in the sense that nodes under attack do not provide control response and therefore these nodes are less critical because retaining observability rather than controllability is the core objective A further example of self-organization in the smart grid domain refers to a communication network which responds to data congestion management and reconfiguring the architecture in response as presented by Zhang *et al.* [13].

The work documents a pathing methodology for dynamically routing messages through the architecture. However as in the previous example, control functions are not considered, nor is there an assessment of the self-organizing approach from the perspective of a cyber-physical evaluation. The research presented by the authors of this paper differs in its application of self-organization through the involvement of a physical control problem and the application of analysis through the medium of an integrated cyber-physical evaluation framework.

C. Implementation

The proposed SOA is composed of three operational stages: Initialization, Performance Monitoring and Decision Making. The SOA is formed from a series of java based agents via the JADE agent platform connected to a distribution network model in Matpower. Both elements of the simulation are connected through interactions managed by a Gateway Agent.

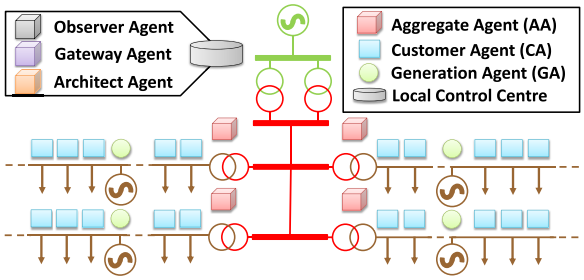

Fig. 2. Network Diagram.

The modeled distribution network consists of 340 domestic smart-metered customers and 4 10MW PV installations across four radial LV feeders. The agent population forming the SOA contains a range of agent classifications: Customer and Generation agents (CAs and GAs respectively) are responsible for monitoring demand and generation and performing local voltage monitoring. All CAs and GAs publish updates to a layer of Aggregation Agents (AAs). The AAs aggregate data from CAs and GAs they are connected to, and respond to control requests from the CAs. Each of the AAs transmits aggregated demand and generation to a central Observer Agent which builds a global view of the network data. Further agents include an Architect Agent which is responsible for processing performance monitoring data and hosts the fuzzy decision-making engine. Finally a Gateway Agent orchestrates the connection to the power system model in Matpower, coordinating the information exchange between both aspects of the integrated platform. Fig. 2 presents the structure of the distribution network and illustrates the placement of agents in relation to the physical layer of the simulation. Connections are not depicted between agents as they are not predetermined and are a factor of the initialization stage.

1) Initialization: Stage one of SOA operation involves forming connections between the CAs/GAs and the AAs. To determine a preferred connection, each CA and GA ranks potential connections based on how quickly each AA responds to a discovery message. This uses a method similar to the mechanism applied by Ojha *et al.* [11].

Each AA has limited connection capacity, if all AAs cannot accept further connections remaining CAs and GAs will be declared isolated. Isolated agents appeal to the Architect agent to request additional AA resource through either activating dormant AAs or promoting CAs into aggregation roles. A further element of the initialization stage is the assignment of substitute agents; a substitute agent is a CA selected by an AA which can be called upon to replace it if the AA becomes unresponsive or fails. Substitutes are selected once all CAs and GAs are connected, and is based on the concept presented by Climent *et al.* [10]. An AA will select a substitute agent by choosing the connected CA with the lowest volume of communication traffic. CAs are initially developed with the internal functions and data structures to assume AA responsibilities. Such functions are disabled unless activated by an instruction from the Architect agent.

TABLE I
PERFORMANCE METRIC THRESHOLDS

Metric	*Limit*	*Rationale*
Maximum Data Flow	15kB/s	Assuming the use of ZigBee technology for communication as per the smart meter specification [40], and assuming an effective throughput rate of 120kbps [41].
Minimum Data Flow	3kB/s	Underutilization set at 20% of the upper limit
Congestion	250 messages	Congestion measured as agent queue size, limits set after calibration testing
Response Time	1.5s	Response time between CAs and AAs, threshold set after calibration testing
Response timeout	10s	Responses are declared missed after three CA update messages, spanning 10s

It is possible for an initialization stage to fail to be executed successfully or to take too long to complete. The self organizing system has some contingencies built into it which mitigate this risk. One of the causes for a failure to initialize the system could be a lack of sufficient aggregational capacity. If this occurs the isolated agents contact the GA and request an increase in aggregational capacity. Fig. 4 provides an indication of how the scale of the multi agent architecture, number of CAs, affects the ability of the system to successfully initialize in an appropriate period of time. The voltage control scheme waits for 180 seconds after a voltage excursion before to ensure the problem is sustained before taking action. Therefore 180 seconds can be taken as an upper bound on the time permitted for initialization. It can be seen in Fig. 4 that when the customer agent population reaches 2300 there is a risk that initialization takes longer than would be acceptable. Therefore an area of network with more than 2300 participating customers would need to be controlled by multiple MAS clusters with distinct initialization groupings.

2) Performance Monitoring: After completing initialization, the SOA enters a performance monitoring stage. Each agent measures a set of local parameters including control performance, message congestion, data flow, unresponsiveness and response times. Each parameter is accompanied by a threshold value to determine if the agent is experiencing performance degradation; these thresholds are documented in Table I. All thresholds were determined through a combination of experimental results, expert knowledge and smart meter specification data. If an agent observes a performance metric operating outside of the threshold, an error report is submitted to the Architect Agent. Each error report contains the location of the violation, its severity with respect to the threshold, along with further details documenting the nature of the error. The Architect agent is responsible for collating all the error reports and calculating the computational burden indicator. Computational burden is calculated using equations 1-3. Where sum of the error severities for each aggregate $(1-\mathrm{n})$ is divided by the number of aggregates, the same process applies for customer agent $(\mathrm{c}_1-\mathrm{c}_\mathrm{n})$. This is process is applied for all error types $(\mathrm{et}_1-\mathrm{et}_\mathrm{n})$ to define an overall system wide burden indicator.

As the burden indicator is a combination of several performance metrics it therefore is represented as a dimensionless quantity The rate of change of the burden indicator is also calculated as a method of assessing whether the error state is improving or deteriorating. If the burden indicator determines that the error state of the network is significant and that rate of change indicates it is a persistent event, the decision-making engine is triggered.

$$B_{Aggregate} = \frac{\sum_{Agg_n}^{Agg_1} (Error\ Severity)}{Number\ of\ Aggregates} \tag{1}$$

$$Burden_{Cust} = \frac{\sum_{C_n}^{C_1} (Error\ Severity)}{Number\ of\ Customers} \tag{2}$$

$$B_{Overall} = \frac{\sum_{et_n}^{et_1} \left(B_{cust} + B_{Aggregate}\right)}{Number\ of\ Error\ Types}. \tag{3}$$

3) Decision Making Engine: Decision Making in the SOA is centered on a fuzzy based decision-making engine supported by decision tree analysis. A fuzzy system has been implemented due to its applicability in non-linear systems of high uncertainty such as in the case of a cyber-attack event involving a human adversary who can behave unpredictably. Furthermore the ambiguity present in the calculation of a computational burden indicator across multiple metrics with multiple units and thresholds is more applicable to a fuzzy centered application.

The fuzzy element of the decision-making engine computes a recommendation for an architectural transition based on the following stages:

Stage 1 (Connection Balancing): A stage 1 transition rebalances connections, AAs with a high number of connections are asked to transfer connections to those with fewer connections. The aim of the transition is to evenly distribute communication between the AAs.

Stage 2 (Agent Substitution): Each AA selects a substitute during the initialization stage.

A stage 2 transition is a predominantly localized event, where a targeted AA is replaced by its designated substitution. If the error state is not localized the Architect will activate a single dormant AA or promote one CA into an aggregation role.

Stage 3 (Dormant Agents): A finite number of dormant AAs are included in the architecture at start-up. These AAs have no active role in the architecture but listen for activation messages. In stage 3, all available dormant agents are activated.

Stage 4 (Agent Promotion): A stage 4 transition involves creating a second AA tier, a number of AAs in the original tier are promoted up to a higher AA tier, those promoted AAs are then replaced by promoted CAs.

Three computational burden levels were discerned based on experimental date and expert knowledge of the system, a similar approach was applied to the rate of change of burden. The membership functions are detailed through the use of equation (4), where x_1 refers to the computational burden membership function and x_2 relates to the rate of change equivalent. F refers to the fuzzy sets with parameters a-d as documented in Table II, the equation also applies to sets with

TABLE II
FUZZY INPUT AND OUTPUT DATASET

Fuzzy Sets & MF Parameters	a	b	c	d
$\boldsymbol{F}_{\mathbf{1},\{1,2,3\}}$ Burden: Low	0	100	250	350
$\boldsymbol{F}_{\mathbf{1},\{4,5,6\}}$ Burden: Med	250	350	500	600
$\boldsymbol{F}_{\mathbf{1},\{7,8,9\}}$ Burden: High	500	600	800	Any x > 800
$\boldsymbol{F}_{\mathbf{2},\{1,4,7\}}$ Rate of Change: Declining	Any x < -5	-5	-5	0
$\boldsymbol{F}_{\mathbf{2},\{2,5,8\}}$Rate of Change: Flat	-5	0	0	5
$\boldsymbol{F}_{\mathbf{2},\{3,6,9\}}$ Rate of Change: Rising	0	5	5	Any x > 5
$\boldsymbol{G}_{\{1,3\}}$ Transition: Stage 1	0	0.125	0.25	0.375
$\boldsymbol{G}_{\{2,4,6\}}$ Transition: Stage 2	0.25	0.375	0.5	0.625
$\boldsymbol{G}_{\{5,7,9\}}$ Transition: Stage 3	0.5	0.625	0.75	0.875
$\boldsymbol{G}_{\{8\}}$ Transition: Stage 4	0.75	0.825	1	Any y > 1

TABLE III
DECISION MAKING ENGINE RULE SET

Burden Indicator	*Rate of Change*	*Decision*
Low	Declining	No Action
Low	Flat	Stage 1
Low	Rising	Stage 2
Medium	Declining	Stage 1
Medium	Flat	Stage 2
Medium	Rising	Stage 3
High	Declining	Stage 2
High	Flat	Stage 3
High	Rising	Stage 4

the notation G. Equation (5) documents illustrates rule firing, equation (6) defines the aggregation process where y_T refers to the transition recommendation. Finally equation (7) defines the defuzzification stage. Table III presents the rule set for the decision-making engine.

$$\mu_{F_{i,l}}(x_i) = \begin{cases} \frac{x_i - a_{F_{i,l}}}{b_{F_{i,l}} - c_{F_{i,l}}} \ \textit{if} \ a_{F_{i,l}} < x_i < b_{F_{i,l}} \\ 1 \ \textit{if} \ b_{F_{i,l}} \leq x_i < c_{F_{i,l}} \\ \frac{d_{F_{i,l}} - x_i}{d_{F_{i,l}} - c_{F_{i,l}}} \ \textit{if} \ c_{F_{i,B}} \leq x_i < d_{F_{i,l}} \\ 0 \ \textit{otherwise} \end{cases} \tag{4}$$

$$f_l(\mathbf{x}) = \prod_{i=1}^{p} \mu_{F_{i,l}}(x_i) \tag{5}$$

$$\mu_B(y_T) = \max\left(f_1(\mathbf{x}) \prod_{j=1}^{N} \mu_{G_1}(y_j), f_9(\mathbf{x}) \prod_{j=1}^{N} \mu_{G_9}(y_j) \right) \tag{6}$$

$$y_c(\mathbf{x}) = \frac{\sum_{j=1}^{N} y_T \mu_B(y_T)}{\sum_{j=1}^{N} \mu_B(y_T)} \tag{7}$$

As previously indicated the values in Table II were attained through experimentation combined with expert knowledge arising from previous work in MAS development. Therefore, this is not considered to be an optimized fuzzy implementation, and further improvements could be attained through undergoing optimization and function tuning techniques. The architect has the power to over-ride a recommendation made by the decision-making engine if it is not feasible based on the location and/or the distribution of the error reports. In which case the Architect will perform an alternative transition. For example if the decision-making engine recommended a stage 2 transition and the Architect determines that the issue is more widespread replacing an AA would be ineffective. Therefore, a single dormant agent will be activated or a single CA promoted if no dormant AAs are available. Each transition decision is independent to its predecessor, and do not necessarily have to be completed in sequence. For example a stage four transition may be followed by a lower stage transition depending on the impact the previous decision had on the computational burden indicator. Equally a stage four transition may be the first recommendation from the decision-making engine based on the severity of the attack event. It should be noted that a transition event is a response to an emerging state within the SOA and therefore does not aim to produce an optimal configuration. The aim is to maintain system functionality and react to the decisions made by an attacker which cannot be pre-determined. For example the configuration created following a stage four transition, includes multiple agents performing functions beyond their initial responsibilities – i.e., CAs acting as AAs. These therefore will experience additional computational load and the potential for component failure.

Consequently preemptively launching the SOA in a post stage four configuration for persistent operation may be more damaging. Following a completed transition, the Architect enters a stand-off period within which no further transitions are triggered. Lower stage transitions result in shorter stand-off times whereas higher stage transitions are given a longer period. The purpose of the stand-time is to reduce the possibility of the attacker exploiting the properties of the SOA. For example, a Reduction of Quality (RoQ) attack [41], aims to trigger continuous restructuring actions which would disrupt the data collection and control objectives of the SOA.

Error reports are still collected during the stand-off period, but no further architectural transitions will take place. The Architect also clears error expired error reports to prevent them from factoring in future decisions.

IV. EVALUATION METHOD

To evaluate the effectiveness of the SOA, it was relevant to compare its resilience to an attack event in comparison to a static architecture. The selected static architecture represents the typical design approaches present in literature, a three tier structure with customer/generation agents on the bottom tier, local controllers assigned at one per feeder on the central tier, and a local control centre responsible for the network under observation. The objective of the evaluation was twofold, firstly to examine the ability of the SOA to perform the control objective under the pressure of a denial of service attack. Secondly to reduce the computational impact of the attack and illustrate the wider applicability of the SOA.

A. Network Conditions

The distribution network – as presented in Fig. 2 – is heavily loaded with limited available local generation, therefore is vulnerable to under-voltage states. Control is provided through demand side response in the form of customer load shedding. Approximately 25% of total demand is controllable. Upon observing a persistent voltage deviation exceeding 180s,

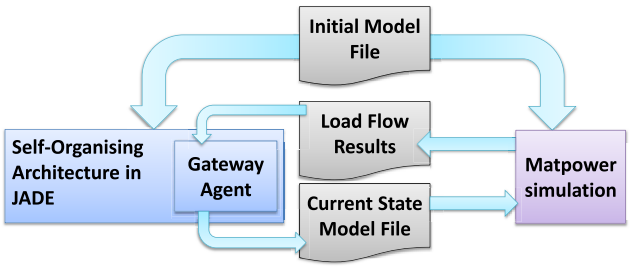

Fig. 3. Integrated Test Platform Structure.

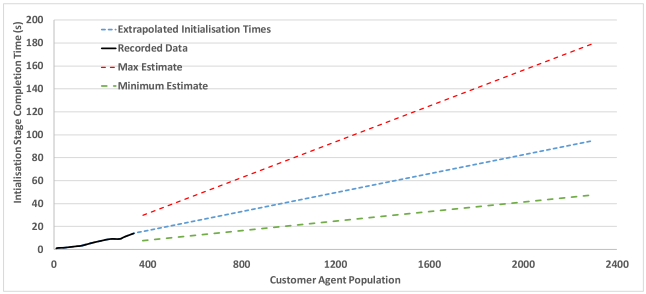

Fig. 4. Estimated Initialization Stage Completion Times.

a CA would contact its associated AA with a control request. In response, the AA would contact agents on the same feeder as the deviation which it is associated with and issue a control signal. CAs performing load shedding periodically ask their AA, if that shedding process is required. If no response is received within 30 seconds, the CA assumes that control is not required and cancels all shedding operations. To assess the severity of the voltage deviation during an attack difference between the measured voltage and the nominal limit of 0.94pu was multiplied by the length of time that measurement was valid. Repeated for each voltage measurement underneath the threshold value as represented by equation (8). Where t_d represents the timestamp of a measurement during the deviation, V_n is the nominal minimum voltage and V_a is the actual measured voltage

$$\sum_{t_{dn}}^{t_{d1}} (V_n - V_a)(t_{t+1} - t_d) \tag{8}$$

The maximum deviation references an instance when no control actions are performed for voltage control, and each deviation event recorded during a simulation is determined as a percentage of the maximum deviation event.

B. Integrated Platform

A further contribution of the research was the development of a test platform which connected the SOA represented in JADE with an electrical model in Matpower as illustrated in Fig. 3. An initial model file is supplied both Matpower and the SOA detailing the starting state of the network, and the stating voltages are written to a results file.. During a simulation the Gateway Agent (GWA) is supplied with demand and generation data from the agent population. The GWA maintains a copy of the initial Matpower model file and updates it with data retrieved from the agents. Periodically the GWA triggers a Matpower load flow using the updated model file through a command line script.

A MATLAB script creates a result file which contains an updated set of bus voltages, which is read back into the SOA via the GWA. This iterative process creates a cyber-physical simulation of the network and the agents involved in operating the SOA.

C. Attack Modeling

The DoS attack was deployed using compromised CAs as attackers involving 6% to 24% of the CA population. As an attacker, the CA would transmit a volume of attack traffic to its AA aiming to disrupt control signals. Because CAs require continuous interaction between themselves and the AA to maintain control, the attack aims to severe that connection and trigger control deterioration. The DoS attack differs from a generic congestion problem or network disabling event similar to those indicated in [13] and [14] it is a specifically targeted event. Additionally network congestion through legitimate traffic can be forecasted at points of peak load, whereas a DoS event is not predictable due to the intent of the attacker. The examined attacks were based on the DoS approaches as described by Luo *et al.* [42] and Kuzmanovic and Knightly [43]. CAs are instructed to launch the attack during the under-voltage event to specifically target the control process.

The attack formats examined are as follows:

Burst Attack: A Low Rate attack acts as a DoS attack where the attacker does not sustain the attack traffic. In this format the attack is sustained for 250 seconds and is scheduled to take place as the controllers are act to resolve the voltage deviation.

Sequential Attack: A sequence of each aiming to disrupt the initial control action requests and subsequent periodic load curtailment checks made by the CAs.

Continuous Low Rate Attack: This attack format presents with continuous stream of attack traffic, the stream is triggered at the point of performing voltage control and endures to the end of the simulation.

Static Attack: Each of the previously listed attack formats was firstly implemented in the form of a static attack. Where the DoS attack performed by an adversary does not react to reconfigurations triggered by the architect. A CA attacker will transmit attack traffic to its original intended target regardless of any reconfiguration actions.

Adaptive Attack: In contrast to the static attack, the adaptive attack involves the attacker selecting an alternative target if an architectural transition is imposed. The attacker listens for any changes in the communication route for legitimate traffic and redirects the attack traffic accordingly. The performance of the SOA is evaluated with respect to control performance and computational burden, to illustrate that the SOA can prevent control deterioration which would be present under a static architecture.

V. Results

Several elements of the system performance have been evaluated in response to the core objectives of a self-organizing

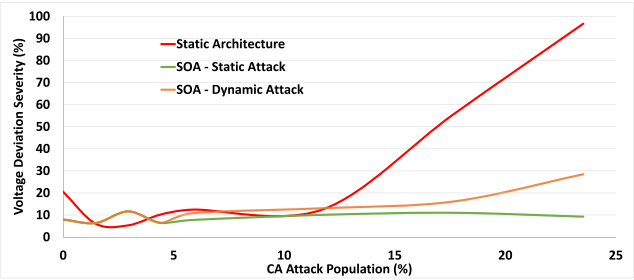

Fig. 5. Deviation Severity under Increasing Attack Strengths.

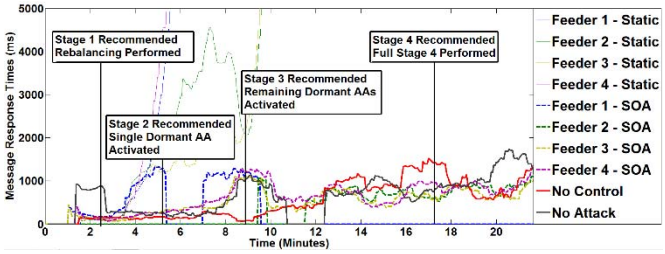

Fig. 6. Decision Making during a Continuous Attack with 24% CA Involvement.

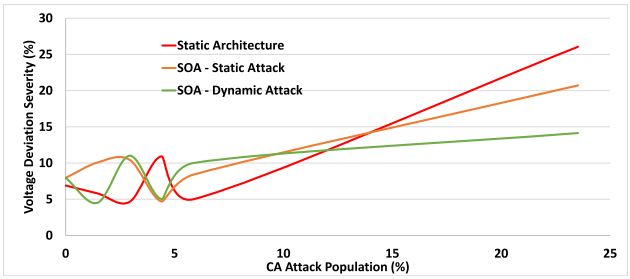

Fig. 7. Deviation Severity during Sequential Attacks.

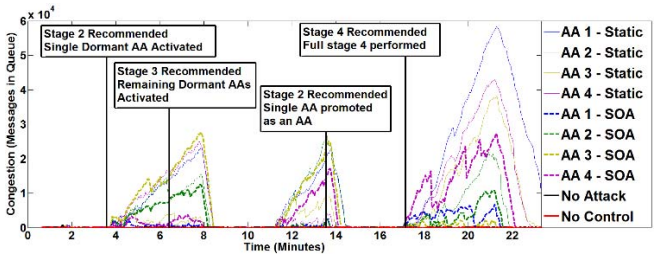

Fig. 8. Congestion Data during an Adaptive Sequential Attack with 24% CA Involvement.

architecture. The first consideration is with respect to scalability. While scalability can be notably influenced by the evolution of an attack event the assessments have been made in the context of the evaluation stage of operation. Fig. 4 documents estimated completion times of the initialization stage extrapolated from measured data up to 340 customer agents. The figures are scaled to the customer populations examined in the previous work as referred to in [26]. The data indicates that a fundamental element of the SOA, does not experience exponential growth in computational time with an increasing population and therefore the proposed system can be deemed scalable. These results also align with performance evaluations performed on the same MAS platform by Cortese *et al.* [44].

A second element of the performance criteria refers to the resilience against the denial-of-service attack scenarios and the effectiveness in comparison to multi-agent system with a rigid communication architecture. This is considered to be a static architecture. A series of continuous attacks hosted by an increasing number of CA agents was performed with and without the presence of the SOA. The voltage deviation sensitivities during these attacks are presented in Fig. 5. The figure illustrates that for smaller numbers of compromised smart-meters the strength of the attack is not significant enough to exacerbate the voltage deviation. However with stronger attacks the control capability becomes increasingly compromised – with 24% of CAs transmitting attack traffic the voltage deviation reaches 96% of the severity in the complete absence of control. Therefore, indicating that the attack effectively disables the voltage control capabilities of the MAS. In comparison the SOA does not experience the same control degradation at the same attack strength in either presence of either a static or dynamic DoS attack. To examine the role of the SOA in minimizing the extent of the voltage deviation it is important to consider the actions of the decision -making mechanism.

Fig. 6 presents the transition events triggered by the architect agent over the course of the simulation mapped against the message response time data for each feeder. Without the SOA the response times between feeders 1 and 2 and their CA population raise to over 8 seconds 4 minutes into the simulation – demonstrating the impact of the attack without SOA intervention. This severance of the communication between controller and customer is the source of the control loss identified in the previous figure. Contrastingly the SOA initially performed a rebalancing action, followed by deploying the dormant AA population and finally a Stage 4 tiered promotion. Demonstrating that the SOA can continually adapt to the attack situation through collecting performance monitoring information and decision-making. As a result response times were managed through a reduction in computational burden. A second example considered a set of sequential attacks presented in Fig. 7, in contrast to the continuous attacks the deviation severity across the same attack population is less significant. Therefore, the potential improvements in control performance through the SOA are reduced – indicating that the relevance of the SOA is dependent on the severity of the attack and its disruptive potential. Attacks with less than 15% CA involvement utilizing a sequential strategy do not significantly influence the control potential of the MAS and therefore performing transitional events may be an overreaction. Fig. 8 illustrates the data congestion present during the most severe of the sequential attacks.

This indicates the source of both the improvements made by the SOA and the differing consequences of a sequential attack in comparison to a continuous event. Each peak in the figure represents one of the bursts of attack traffic during the attack, the time between bursts allows each controller to clear its message queue and therefore deliver control messages to the

CA population. The SOA is able to reduce the peak congestion by over 3,500 messages reducing the computational burden index by 64%. A final attack analysis on individual burst attack events also found that they were significantly less disruptive to the control objective. In addition to preventing control loss and therefore minimizing the severity of the under-voltage condition the SOA was also capable of reducing the computational burden. On average across all examined DoS attack strengths and strategies computational burden was lowered by 86.49%. Consequently, indicating that the SOA can have further applications within smart-grid network management.

VI. Conclusion and Further Work

This paper presents a SOA as a solution to mitigate against a series DoS attacks, which if unattended can compromise data availability and by extension result in control degradation and total control loss. As a DoS attack can be considered one of the most dangerous threats to a power system and a strategy which can influence each layer of the TCP/IP protocol stack, the SOA mechanism represents a valuable contribution.

The developed SOA was able to reduce the control degradation created by the DoS attacks in events involving up to 24% of the customer population. Use of the SOA improved response times between the AA and CA layers by up to 8.2 seconds and reduced congestion by up to 16,000 stored messages. Therefore, the SOA was able to reduce the overall computational burden indicator by 89.6% on average.

Based on the results obtained it can be concluded that the developed SOA and its decision-making engine were functional and effective being capable of maintaining controllability during a DoS attack event. The results demonstrated that the SOA was able to reduce the computational burden and revealed important correlations between correcting issues within the communication layer and the resulting positive impacts on control performance. Reducing the burden at the control layer prevented control deterioration experienced by the static architecture and illustrated further potential applications for the SOA.

The adopted approach leaves room for further research, especially with respect to processing additional cyber-threats which remains an interesting and expanding research topic and where SOA could be one of the defensive tools used. Further work will also examine additional attack strategies, control algorithms and network scenarios. Current results could be further enhanced through the application of machine learning and self-tuning with the decision-making engine.

References

[1] R. Ebrahimy and Z. Pourmirza, "Cyber-interdependency in smart energy systems," in *Proc. 3rd Int. Conf. Inf. Syst. Security Privacy*, vol. 1, 2017, pp. 529–537.

[2] J. Vijayan. (Jul. 26, 2010). *Computerworld*. Accessed: Jun. 30, 2016. [Online]. Available: http://www.computerworld.com/article/2519574/security0/stuxnet-renews-power-grid-security-concerns.html

[3] A. Giani *et al.*, "Smart grid data integrity attacks," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244–1253, Sep. 2013.

[4] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[5] G. Cisotto and L. Badia, "Cyber security of smart grids modeled through epidemic models in cellular automata," in *Proc. IEEE 17th Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, Coimbra, Portugal, 2016, pp. 1–6.

[6] K. R. Davis *et al.*, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sep. 2015.

[7] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sep. 2015.

[8] Y. Mo *et al.*, "Cyber—Physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[9] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, Mar. 2015.

[10] S. Climent, J. V. Capella, N. Meratnia, and J. J. Serrano, "Underwater sensor networks: A new energy efficient and robust architecture," *Sensors*, vol. 12, no. 1, pp. 704–731, 2012.

[11] T. Ojha, M. Khatua, and S. Misra, "Tic-Tac-Toe-Arch: A self-organising virtual architecture for underwater sensor networks," *IET Wireless Sensor Syst.*, vol. 3, no. 4, pp. 307–316, Dec. 2013.

[12] W. Narzt, U. Wilflingseder, G. Pomberger, D. Kolb, and H. Hortner, "Self-organising congestion evasion strategies using ant-based pheromones," *IET Intell. Transp. Syst.*, vol. 4, no. 1, pp. 93–102, Mar. 2010.

[13] Y. Zhang *et al.*, "A multi-level communication architecture of smart grid based on congestion aware wireless mesh network," in *Proc. North Amer. Power Symp.*, Boston, MA, USA, 2011, pp. 1–6.

[14] H. Lin *et al.*, "Self-healing attack-resilient PMU network for power system operation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1551–1565, May 2018.

[15] F. Cohen, "The smarter grid," *IEEE Security Privacy*, vol. 8, no. 1, pp. 60–63, Jan./Feb. 2010.

[16] *Enhancing Distribution Resiliency Opportunities for Applying Innovative Technologies*, Elect. Power Res. Inst., Palo Alto, CA, USA, 2013.

[17] *Analysis of the Cyber Attack on the Ukranian Power Grid*, Electricity Inf. Sharing Anal. Centre, Washington, DC, USA, 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[18] B. Li, R. Lu, W. Wang, and K.-K. R. Choo, "Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system," *J. Parallel Distrib. Comput.*, vol. 103, pp. 32–41, May 2017.

[19] Y. Yuan, Z. Li, and K. Ren, "False data injection attacks in smart grid," in *Wiley Encyclopedia of Electrical and Electronics Engineering*. Hoboken, NJ, USA: Wiley, 2012.

[20] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[21] P.-Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, "Detection of false data injection attacks in smart-grid systems," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 206–213, Feb. 2015.

[22] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, 2009, pp. 21–32.

[23] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[24] X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.

[25] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," in *Proc. 44th Annu. Conf. Inf. Sci. Syst. (CISS)*, Princeton, NJ, USA, 2010, pp. 1–6.

[26] F. M. Cleveland, "Cyber security issues for advanced metering infrastructure (AMI)," in *Proc. IEEE Power Energy Soc. Gen. Meeting Convers. Del. Elect. Energy 21st Century*, Pittsburgh, PA, USA, 2008, pp. 1–5.

[27] D. Kushner, "The real story of stuxnet," *IEEE Spectr.*, vol. 50, no. 3, pp. 48–53, Mar. 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[28] S. Xu, Y. Qian, and R. Q. Hu, "On reliability of smart grid neighborhood area networks," *IEEE Access*, vol. 3, pp. 2352–2365, 2015.

[29] C. D. Cameron, C. Patsios, and P. C. Taylor, "On the benefits of using self-organising multi-agent architectures in network management," in *Proc. Int. Symp. Smart Elect. Distrib. Syst. Technol. (EDST)*, Vienna, Austria, 2015, pp. 335–340.

[30] M. J. Dolan *et al.*, "Northern Isles new energy solutions: Active network management stability limits," in *Proc. 3rd IEEE PES Int. Conf. Exhibit. Innov. Smart Grid Technol. (ISGT Europe)*, Berlin, Germany, 2012, pp. 1–9.
[31] V. Rigoni, *Deliverable 3.7 'Characterisation of LV Networks'*, Univ. Manchester, Manchester, U.K., 2014. [Online]. Available: http://www.enwl.co.uk/docs/default-source/future-low-voltage/university-of-manchester-appendix-j.pdf?sfvrsn=2
[32] *Low Carbon Networks Fund Full Submission Pro Forma*, Low Carbon Netw. Fund, London, U.K., 2011. [Online]. Available: https://www.ofgem.gov.uk/ofgem-publications/91889/appendix7publish.pdf
[33] M. S. E. Moursi and H. Mehrjerdi, "A coordinated control strategy of voltage regulation in power system based on multi-agent system," *Ind. Eng. Manag.*, vol. 3, no. 2, p. 128, 2014.
[34] T. Nagata, Y. Tao, H. Sasaki, and H. Fujita, "A multiagent approach to distribution system restoration," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Toronto, ON, Canada, 2003, p. 660.
[35] J. Zhou, R. Q. Hu, and Y. Qian, "Scalable distributed communication architectures to support advanced metering infrastructure in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1632–1642, Sep. 2012.
[36] L. Jun, Z. Shunyi, Z. Zailong, and W. Pan, "A novel network management architecture for self-organizing network," in *Proc. Int. Conf. Netw. Archit. Stor. (NAS)*, Guilin, China, 2007, pp. 146–154.
[37] G. D. M. Serugendo, M.-P. Gleizes, and A. Karageorgos, "Self-organization in multi-agent systems," *Knowl. Eng. Rev.*, vol. 20, no. 2, pp. 165–189, 2005.
[38] S. Srivastava, S. Suryanarayanan, P. Ribeiro, D. Cartes, and M. Stcurer, "A conceptual power quality monitoring technique based on multi-agent systems," in *Proc. 37th Annu. North Amer. Power Symp.*, Ames, IA, USA, 2005, pp. 358–363.
[39] *ZigBee Smart Energy Profile Specification*, ZigBee Alliance, Davis, CA, USA, 2008.
[40] M. O. Farooq and T. Kunz, "On determining bandwidth usage threshold to support real-time multimedia applications in wireless multimedia sensor networks," in *Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Barcelona, Spain, 2013, pp. 401–406.
[41] M. Guirguis, A. Bestavros, and I. Matta, "Exploiting the transients of adaptation for RoQ attacks on Internet resources," in *Proc. 12th IEEE Int. Conf. Netw. Protocols (ICNP)*, Berlin, Germany, 2004, pp. 184–195.
[42] J. Luo *et al.*, "On a mathematical model for low-rate shrew DDoS," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1069–1083, Jul. 2014.
[43] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks and counter strategies," *IEEE/ACM Trans. Netw.*, vol. 14, no. 4, pp. 683–696, Aug. 2006.
[44] E. Cortese, F. Quarta, G. Vitaglione, and P. Vrba, "Scalability and performance of JADE message transport system?" *J. Anal. Suitability Holonic Manuf. Syst.*, vol. 3, no. 3, pp. 52–65, 2002.

Calum Cameron received the B.Sc. degree (First Class Hons.) in computer forensics from Northumbria University in 2010, the M.Sc. degree (with Distinction) in advanced software engineering from Durham University in 2013, and the Ph.D. degree in self-organising multiagent architectures for smart grid cyber security from Newcastle University in 2017.

Charalampos (Haris) Patsios received the electrical engineering degree from the University of Patras in 2005 and the Ph.D. degree from the National Technical University of Athens in 2011. He is a Lecturer in power systems with the School of Engineering, Newcastle University. He has significant experience in the design, modeling, and control of electrical power systems including energy storage, renewables, and power electronics. His research involves the development of models, grid interfaces, and control techniques for energy storage systems as well as decentralized control in future power networks, working closely with U.K. industry and academia.

Phil C. Taylor (SM'12) received the Engineering Doctorate degree in intelligent demand side management techniques from the University of Manchester Institute of Science and Technology, Manchester, U.K., in 2001. He joined Newcastle University, Newcastle upon Tyne, U.K., in 2013, where he is the Head of the School of Engineering and holds the Siemens Chair of Energy Systems. He is a Visiting Professor with Nanyang Technological University, Singapore. He previously held the DONG Energy Chair in Renewable Energy and was a Director of the Durham Energy Institute.

Zoya Pourmirza received the undergraduation degree in information technology engineering from the Sharif University of Technology and the Ph.D. degree in smart grid information and communication technology (ICT) architecture from the University of Manchester, U.K., in 2015. She then joined the Newcastle University as Research Associate in the Power System Group, where she is a Research Associate. Her research is concerning about designing an ICT architecture for the smart electrical grid with emphasis on making the ICT infrastructure energy aware. She also investigates cyber security aspects of the smart grid, focusing on data integrity and availability attack for information in transition in ICT infrastructure of the Smart Energy Systems.