A Characterisation of Smart Grid DoS Attacks

Dilara Acarali[1], Muttukrishnan Rajarajan[1], Doron Chema[2], and Mark Ginzburg[2]

[1] School of Mathematics, Computer Science & Engineering. City, University of London. London, UK.
{dilara.acarali.2, r.muttukrishnan}@city.ac.uk
www.city.ac.uk/about/schools/mathematics-computer-science-engineering
[2] Technical Team, L7 Defense, BeerSheva, Israel
{doron, marik}@l7defense.com
www.l7defense.com/

Abstract. Traditional power grids are evolving to keep pace with the demands of the modern age. Smart grids contain integrated IT systems for better management and efficiency, but in doing so, also inherit a plethora of cyber-security threats and vulnerabilities. Denial-of-Service (DoS) is one such threat. At the same time, the smart grid has particular characteristics (e.g. minimal delay tolerance), which can influence the nature of threats and so require special consideration. In this paper, we identify a set of possible smart grid-specific DoS scenarios based on current research, and analyse them in the context of the grid components they target. Based on this, we propose a novel target-based classification scheme and further characterise each scenario by qualitatively exploring it in the context of the underlying grid infrastructure. This culminates in a smart grid-centric analysis of the threat to reveal the nature of DoS in this environment.

Keywords: Smart grid · cyber-security · DoS · DDoS.

1 Introduction

The digital age has caused an increased dependency on electricity, and consequently, given rise to an increased demand on power systems. As a result, traditional power grids have had to evolve to deal with this inflated demand. A smart grid is a traditional power grid integrated with information communication systems. The former is referred to as the physical or operational technology (OT), and the latter is called the cyber or information technology (IT). In practice, this means that IT networks gather data from field systems and deliver them to a central command centre via local controllers. That data can then be used to regulate physical grid components and to make management decisions.

Whilst this can greatly improve efficiency, the IT network also makes the smart grid more vulnerable to malicious activity by expanding the previously limited attack surface. Grid components are now remotely accessible, and grid processes are now dependent on data flows through communication channels that

can be disrupted. Furthermore, the cyber and the physical systems are highly interconnected and interdependent, meaning that faults or attacks at one point can cause a chain of effect across the wider smart grid.

This work is focused on Denial-of-Service (DoS), a well-known cyber-attack targeting availability, designed to hinder normal system processes. It is popular because, despite being relatively simple, a successful DoS attack can cause a large degree of disruption. DoS attack methodology may consist of a) flooding, where a channel/device is overwhelmed with data, b) the exploitation of vulnerabilities or quirks in systems and protocols, or c) both. A DoS attack launched by multiple dispersed individuals (e.g. in a botnet) is known as Distributed DoS (DDoS). Whilst disruption resulting from physical tampering can also be explored, we consider DoS predominantly as a cyber threat.

DoS attacks in conventional networks are well-studied, but the smart grid has particularities that influence both methodology and results. In this paper, we first identify and then characterise smart grid DoS scenarios to build up a picture of how this threat manifests in this new environment. Identification is achieved via a detailed survey of existing research, which then forms the basis of a new classification scheme organised by potential targets. This differs from conventional approaches and is designed to link targeted grid components with likely DoS attack methods, providing a reference for researchers and defenders. To our knowledge, a survey and classification of smart grid-specific DoS scenarios is novel to this work.

The research presented in this paper is part of the European Union's *Energy Shield* project [1], commissioned in recognition of the energy industry's transition from traditional systems to smart grids. The aim of this project is to develop a defence toolkit for EPES (Electrical Power and Energy System) operators [1] to protect critical infrastructure from cyber-attacks, including DDoS. This work was conducted to provide a foundation of understanding of the smart grid-centric DoS threat on which the project can further build.

The rest of the paper is structured as follows: Section 2 provides a background explanation of smart grid architecture, including domains, flows, and key components. Then, the smart grid DoS research survey is presented in Section 3. Based on the information in 2 and 3, Section 4 presents our classification scheme and characterisations of the identified DoS scenarios. This is followed by the discussion of our findings in Section 5, with an analysis of related works given in Section 6. We then conclude in Section 7.

2 Smart Grids Background

2.1 Smart Grid Domains

The smart grid follows a domain model architecture, which means it is split into multiple domains, each handling a different function. A domain will generate/process either power flows (in the OT), communication flows (in the IT), or both. Generally, data on power flows is collected and shared as communication

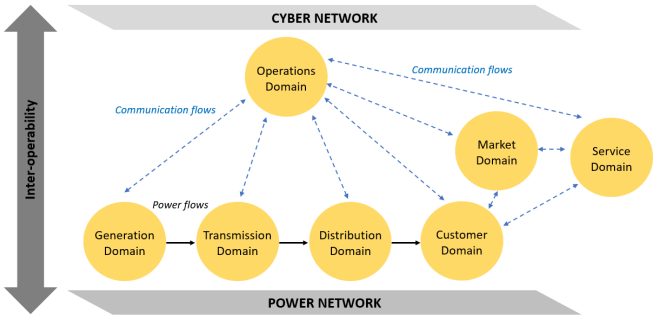

Fig. 1. Smart grid domains.

flows. Fig. 1 provides an illustration of the core domains as they relate to each other and the flows between them. Note that this paper focuses on communication flows as the main target of DoS attacks, but the characteristics of these are influenced by the nature of the underlying power flows.

The core domains of the traditional power grid, responsible for the production and delivery of electricity as a utility, are described first. These are the ones that contain power flows. The Customer domain deals with the delivery of power to customer premises. It also handles the collection of usage data. Power is received from the Distribution domain, which is responsible for dissemination. This domain also transforms the power received from the Transmission domain, which is where bulk energy is carried between geographically distributed locations (e.g. a power plant and a city). The Generation domain houses power plants where electricity is 'produced'. If distributed power generation exists (i.e. customers generate their own electricity), this is also handled within the Customer and Distribution domains.

The rest are the communication-focused domains. Operations is the main control hub and the core of the communication network, responsible for the collection of monitoring data and the dissemination of control commands. The Service domain houses the providers who deliver electricity as a utility, whilst the buying/selling of electricity is handled within the Markets domain. Both Service and Markets make use of the IT to provision services and to bill customers. However, it should be noted that there is a separation between the IT that controls the grid, and the corporate TCP/IP networks of energy companies and service providers.

2.2 Smart Grid Structure

The traditional power grid (i.e. the OT) is hierarchical in the way it transmits and distributes electricity to users. One or more power plants generate electricity. This is then carried in bulk through heavy-duty transmission lines to many geographically dispersed substations. Here, transformers convert (i.e. step-down) and transfer energy to distribution lines, which then branch out to deliver power

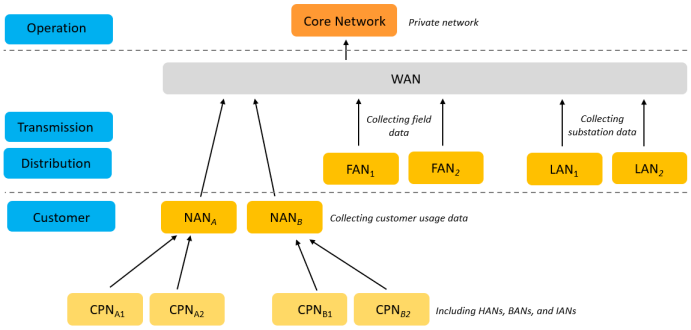

Fig. 2. Smart grid IT network hierarchy with CPNs (Customer Premise Networks).

to a large number of individual customer premises. Hence, there are a larger number of component systems at the bottom then at the top, which means that a single problem higher up in the power hierarchy affects many systems lower down.

The IT network is also hierarchical. For a given region and/or provider, a single core management system, such as SCADA (Supervisor Control and Data Acquisition), contains various master controls to monitor, analyse, and regulate grid operations. This core network receives inputs from distributed monitoring devices (like RTUs and PLCs, described in the next sub-section) sitting in FANs (Field Area Networks), NANs (Neighbourhood Area Network) and substation LANs (Local Area Networks) operating throughout the Generation, Transmission, and Distribution domains. NANs amalgamate smaller customer networks, including HANs (Home Area Networks), BANs (Business Area Networks), and IANs (Industry Area Networks). Each contain devices that connect to upload usage data. As with the OT, the IT hierarchy means that higher level issues impact a large number of lower level systems. Furthermore, there is a variation in DoS attack surface (smaller at the top, bigger at the bottom).

In addition to this, connectivity and dependency exist between the IT and OT, which means that malicious activity in one will have some influence on the other. In other words, assuming that DoS attacks are targeted at IT devices/flows, when some function of the IT network is denied, there will be a corresponding impact, related to that function, on the OT. Furthermore, disruption to a particular grid process can have subsequent effects on other processes, and may escalate into general grid instability. This is a unique characteristic of critical infrastructures, as DoS within conventional IT networks does not typically have the potential for this level of widespread disruption.

2.3 Smart Grid Components

Within the IT network, there are a number of sub-systems responsible for different grid processes. The key sub-systems are:

Systems	Domains	Function
Smart Meter	-Customer	Located in customer premises, collects usage data for operations (via the AMI) and provides pricing information to users.
Remote Telemetry Unit (RTU)	-Distribution -Transmission -Generation	Located in substations, collects data on grid processes from PLCs for automated monitoring and control processes.
Phasor Measurement Unit (PMU)	-Distribution -Transmission -Generation	Located in substations, collects data on electrical phasor patterns for synchronisation of grid supply and demand.
Programmable Logic Controller (PLC)	-Distribution -Transmission -Operations	Field device, collects telemetry data on grid processes, communicated to RTUs and LFC to generate control signals.
Master Telemetry Unit (MTU)	-Operations	Part of SCADA or WAMS, processes data received and aggregated from RTUs.
Phasor Data Concentrator (PDC)	-Distribution -Transmission -Generation -Operations	Part of SCADA or WAMS, processes data received and aggregated from PMUS.
Load Frequency Control (LFC)	-Generation	Located alongside generators, minimises fluctuations in energy input and output for frequency balance.
Supervisory Control & Data Acquisition (SCADA)	-Operations	Control system, responsible for manipulating grid topology, monitoring processes, and maintaining functionality.
Wide Area Management System (WAMS)	-Operations	Control system, uses information gained from PMU/PDC data to monitor and react to grid instabilities/issues.

Table 1. Smart grid sub-systems and components, their domains, and their functions.

-Advanced Metering Infrastructure (AMI): A two-way communication network between smart meters sitting within customer premises and utility servers in the core network. The AMI enables the collection of usage data (analysed for load forecasting and pricing models), as well as the delivery of relevant customer services.

-Phasor Control: Consists of PMUs (Phasor Measurement Units) which measure electrical signals and monitor phasor patterns, and PDCs (Phasor Data Concentrators) which aggregate and process this data for monitoring, fault response, and command generation. The purpose of this is to ensure that the frequency of the electricity in the grid is synchronised and the grid remains stable.

-Telemetry Control: Consists of RTUs (Remote Telemetry Units, distributed across the domains), which collect telemetry data from grid components, and MTUs (Master Telemetry Units, connected to core systems), which receive that data and process it for management and topology manipulation. This supports

efficient power generation and transfer. RTUs connect multiple PLCs (Programmable Logic Controllers), which connect to field devices.
-Load Frequency Control: Consists of PLCs (that connect to field devices) and RTUs which collect data on the performance of various processes. This is communicated to LFCs (Load Frequency Controls), which use the data to manage generators to maintain a stable frequency in the grid.
-Core Control Systems: Includes SCADA (Supervisor Control and Data Acquisition) systems and WAMS (Wide Area Management Systems), which act as the central management point for the grid, where all data is aggregated, processed, and used for human-lead decision-making and for automatically generated controls.

Table 1 provides a summary of typical sub-systems and components, which domains they sit in, and what they do. Note that this list is not exhaustive. For the scope of this paper, we have focused on the most common sub-systems which rely on communication flows. Other systems include those responsible for pricing models, for distributed power generation management, and external data systems used for load prediction (e.g. weather forecasts).

3 Smart Grid DoS Survey

The purpose of this survey is to answer the following research question: *According to the literature, what are the DoS attack possibilities in smart grids, given the smart grid's unique characteristics?* The answer to this question must consider attack method, attack target, and attack impact. The survey methodology used is as outlined in [4], and the review protocol was to search IEEEXplore, Science Direct, and Google Scholar with a set of DoS and smart grid search term pairs. Specifically, we aimed to identify recent works that defined, modelled, simulated, or discussed DoS scenarios. Note that SCADA or WAMS are not considered, as these systems are common across critical infrastructures and are considered a separate field of study. The scenarios identified in the surveyed works are summarised here.

Wang et al. (2017) [23] explored the adversarial interaction between smart grid defenders and attackers, anchored on an AMI DDoS attack. The AMI is modelled as a tree with many smart meters connecting to aggregators in layers. Traffic from the meters travels up these layers to a base station, which then relays it to the AMI core. In this study, the attacks were targeted at smart meters and aggregators, assuming the attack source to be a botnet. The authors found that, depending on where the target sits, certain communication paths become saturated, with nodes attached to these paths consequently being knocked offline. Meanwhile, the AMI's tree structure eventually causes "downstream" nodes to lose core connectivity [23]. Honeypots embedded within the AMI core were used to derive optimal attack and defence strategies.

As with [23], Guo and Ten (2015) [8] also studied a botnet-driven AMI DDoS scenario. They created a two-staged model combining botnet formation and attack launch. Three actor categories were considered: attackers, victims, and

agents (i.e. smart meters converted into bots). The authors posited that it is reasonable to assume that a population of smart meters will have similar vulnerabilities, and hence, will be susceptible to the spread of an automated malware targeting firmware or communication functions [8]. They simulated a UDP flood against a 2-layer AMI topology, with each bot generating packets at a rate of 2Mbps [8] and reported that growth in the bot population directly correlated with an increased number of dropped packets and longer end-to-end delays [8].

Similarly, Sgouras et al. (2017) [20] investigated the AMI impact of a botnet-launched DDoS attack. They modelled the AMI as multiple residential smart meters connected to a central control server, and posited that the Internet is a likely channel for communication between control servers and aggregators. Based on this, they suggested that a botmaster could sniff traffic to determine the server IP and then use a botnet (external to the smart grid network) to launch a TCP SYN DDoS attack at great scale. Using this proof-of-concept, the authors were able to demonstrate how Internet-connectivity exposes the grid to the outside world and can make it susceptible to attacks from remote adversaries.

Asri and Pranggono (2015) [3] also investigated botnet-based DDoS attacks against the AMI. With similar assumptions to [20], they modelled the AMI as a collection of households containing smart meters connecting to a central utility server via the Internet. An external botnet can then connect to the utility server to flood it in a UDP storm attack, targeting many random ports. The server will try to initiate applications on random ports that do not exist and respond with ICMP 'Destination Unreachable' packets [3]. With simulations, the authors showed that the entire grid could be compromised with a large-enough DDoS attack, though the effect on the power supply network was not immediate. Only after the server had been knocked offline was an impact observed.

Sgouras et al. (2014) [19] considered four different AMI DoS setups: 1) DoS on a smart meter, 2) DDoS on a smart meter, 3) DoS against an AMI utility server, and 4) DDoS on an AMI utility server. Comparing the DoS and DDoS scenarios, they found that the targeted smart meter suffered from significantly increased queue lengths under the latter. In fact, they observed that queue lengths reached maximum levels much faster. The DoS attack against the server caused a drop in the number of TCP packets delivered to smart meters, leading to some service degradation. In comparison, the DDoS attack on the server reportedly diminished connections with almost 90% of the smart meters [19].

Hoffman and Bumiller (2019) [9] proposed a special AMI DoS attack called Denial-of-Sleep. This is where a battery-powered device is prevented from entering sleep mode (i.e. a low-power state intended to conserve energy), thereby significantly reducing its lifespan. Smart meters enter sleep mode when they are not forwarding measurement data or receiving traffic from other nodes [9]. Two sleep protocols are identified: S-/T-mode (where the device transmits and waits some time for a response before sleeping) and C-mode (where the device sleeps immediately after completing its transmission). The authors used an abstract version of a TLS (Transport Layer Security) handshake to model Denial-of-Sleep attacks in the context of the C-mode sleep protocol and reported that a small

number of attacks of relatively short length can significantly deplete batteries [9].

Chatfield et al. (2018) [5] studied jamming, which they categorised as a form of DoS used to disrupt the wireless networks within smart grids. They defined two possible scenarios. The first is where a jamming attack produces lots of radio signals on the same frequency as legitimate communications, causing delays and increased latency for control messages. The second is where the degradation caused by a jamming attack interferes with standard protocol processes and leads to constant retransmissions, further congesting the network and, in the case of routing protocols, causing network instability [5]. In their AMI model, they used the received signal strength of nodes to differentiate between normal and attack scenarios, and related attack effectiveness to the distance between attacker and victim nodes.

Pedramnia and Rahmani (2018) [17] explored AMI-based DoS against cellular LTE (Long-Term Evolution) networks. They identified signalling attacks, where bearer assignment is exploited to prevent legitimate use. A malicious bearer request is sent, and once an assignment is made, that bearer is left unused. It expires, triggering another assignment process, and the pattern is repeated. LTE-specific jamming attacks may be possible too. The authors also discussed SMS link saturation, where device user panels (where customers receive updates) are flooded. This drowns out legitimate messages, causes buffer overflows, or leads to delays [17]. Lastly, DoS against NAT (Network Address Translation) systems are highlighted, specifically for NAT64. These include NAT overflow (where malicious mapping requests block legitimate use), NAT wiping (where TCP-RST messages are used to delete mappings), and NAT breaking (where spoofed IPs make NAT requests and ignore server responses, forcing those IPs onto blacklists) [17].

Yi et al. (2016) [27] defined a new AMI DoS technique called the puppet attack. This seeks to exploit the use of DSR (Dynamic Source Routing) and the way that mesh networks are formed. One or more nodes are selected as 'puppets', and receive attack commands. DSR uses route requests (RREQ) and route replies (RREP) to build address lists amongst nodes. The attack makes a puppet node erase addresses from the list, causing path errors [27]. This then triggers another round of path discovery and list building, thereby stopping the network from settling into a routing structure. This contrasts with standard DoS which relies on crafted packets or exhaustion of resources. Meanwhile, puppet attacks undermine the structure and functionality of the mesh itself.

Wei and Kundar (2012) [25] explored DoS attacks targeting communication channels between distributed PMUs and the WAMS. Specifically, the authors suggested that PMU data rates may vary with network congestion. They modelled a hierarchical network covering the cyber (IT) and physical (OT) networks. PMUs in the cyber network collect data on a particular generator node in the physical network. Local controllers obtain data from PMUs to create control signals to be applied to the generator nodes. Generators are grouped into clusters, with a single PMU and local controller in charge of each cluster. Hence, power

Ref	Premise	Target	Impact
[23]	Defender vs. attacker interactions.	AMI	Channel saturation; downstream nodes lose core connectivity.
[8]	Botnet-launched UDP flood DDoS.	AMI	Botnet growth increases dropped packets and end-to-end delays.
[20]	Botnet-launched TCP-SYN DDoS.	AMI	Load fluctuations and system availability diminished.
[3]	UDP storm DDoS against residential AMI.	AMI	Possible complete compromise; delayed impact on power network.
[19]	DoS/DDoS attack impact in the AMI.	AMI	Dropped TCP packets, service degradation, and diminished connectivity.
[9]	Denial-of-Sleep attacks against battery-powered AMI nodes.	AMI	Increased battery depletion in affected nodes.
[5]	Jamming attack detection in wireless networks.	AMI	Delays on legit frequencies; protocol process interruption.
[17]	Signalling, SMS link saturation, and NAT attacks against cellular LTE networks.	AMI	Repeated bearer assignments; reduces devices' interface functionality. NAT-based disruptions.
[27]	Puppet attack against mesh networks.	AMI	Corrupted address lists, causing path discovery cycles.
[25]	Resilient routing model for PMUs-WAMS traffic.	PMUs	Delays/packet dropping within PMU data channels.
[21]	Nash Equilibrium-based DoS-resilient routing.	PMUs	Reduced relay nodes functionality; delays/reduced connectivity.
[28]	Interface and PLC-targeting attacks exploiting query replies.	PLCs	Delays increase with attack length, management SW becomes non-functional.
[14]	DoS switching strategies against LFCs.	LFCs	Attack impact is maximised via start time selection and attack length.

Table 2. DoS types and targets identified by surveyed works.

flow depends on control signals, and control signals depend on PMU data. The DoS attack then targets the PMUs' communication channels with the aim of causing delays or packet drops. The authors used this attack model to propose a flocking-based scheme to route traffic around DoS-affected regions.

Srikantha and Kundur (2015) [21] also studied attacks on PMUs to enhance resiliency against DoS attacks. They modelled the smart grid as a pair of hierarchical, inter-connected directed graphs, populated with relay nodes (RNs) responsible for transmitting data. Some function as PMUs (collecting data) and some as cyber-actuators (sending control signals). At the top of the hierarchy is the root node that transmits control data downstream, whilst PMUs send measurement data upstream. The authors then experimented with DoS attacks that target one or more RNs in the tree. This causes delays and disruption for the downstream/upstream movement of traffic as RNs are rendered non-functional.

As with [25], they proposed a routing system to allow the topology to morph around the attacked nodes.

Yilmaz et al. (2018) [28] explored the possibility of DoS attacks against PLCs, suggesting that a PLC can be targeted both from within and outside of its own IP network, as long as its IP address is known. Furthermore, the authors highlighted that PLCs reply to any queries from any source, further increasing their potential for exploitation [28]. A testbed was built, consisting of PLC devices and some PCs running a) TIA (Totally Integrated Automation) portal management software, b) DoS tools, and c) attack detection systems [28]. Attacks were then simulated against both the PLCs and the TIA portal. The results showed that the PLCs' ping response delay continued to increase the longer the attack was sustained. Meanwhile, the TIA portal became non-functional. The authors noted that the network was quickly disrupted even with a small number of attackers [28].

Finally, Liu et al. (2013) [14] investigated DoS attacks designed to disrupt the delivery of telemetry data from RTUs to LFC systems. This would prevent the LFC from generating accurate command signals for physical grid components, potentially causing further issues. The authors modelled DoS as a switched system and suggested that attacks can have maximum impact if attackers select the optimal switching strategy. They identified this to be a sequential attack over multiple intervals [14]. DoS attacks were simulated with different starting times, revealing that impact was more significant for those launched before power systems have fully converged. This period was therefore highlighted as one of increased vulnerability [14].

The survey is summarised in Table 2 and the findings are analysed in the next section.

4 Smart Grid Denial-of-Service Characterisation

Based on the architecture of smart grids (discussed in Section 2) and the literature survey (presented in Section 3), we propose a set of smart grid DoS scenarios, classified in a target-based structure. This contrasts with existing classification schemes which tend to focus on attack methodology. The main categories are:

- ***A*: Network-Targeting**
  - ***A.1***: Saturation Scenarios (aiming to use up channel resources)
  - ***A.2***: Exploit Scenarios (aiming to manipulate standard processes)
- ***B*: Device-Targeting**
  - ***B.1***: Exhaustion Scenarios (aiming to use up device resources)
  - ***B.2***: Compromise Scenarios (aiming to manipulate a device)

In *A* scenarios, the aim is to disrupt the network itself, either by blocking communications through full consumption of channel capacity (*A.1*), or the blocking of standard operations by preventing normal protocols from functioning as intended (*A.2*). Meanwhile, the aim of *B* scenarios is to disrupt the operation of particular network nodes so that they can be manipulated and cannot function

as normal. This may be achieved by overwhelming the capacity of a device (*B.1*) or by exploiting some vulnerability in it (*B.2*). Note that *B.1* scenarios are similar in concept to *A.1*. In the following, each scenario is described in terms of the smart grid sub-systems that may be targeted, allowing us to consider subsequent impact possibilities given the smart grid's multifaceted and interconnected infrastructure. Key points for effective defence and mitigation are also highlighted.

4.1 Network Saturation Scenarios (*A.1*)

The AMI may use a number of communication technologies, including WiFi, WSNs, cellular networks, or the Internet. Hence, it can be targeted in several different ways. Saturation may be attempted using typical flooding attacks (e.g. ICMP flood, UDP flood, HTTP flood) on any layer of the TCP/IP protocol stack, as seen in conventional networks. This type of scenario was explored by [8] and [3]. Jamming attacks may also be used to similar effect against wireless channels, as cited by [5]. Similarly, where SMS communication is used to push information to device interfaces, SMS link saturation may be employed [17]. Therefore, *A.1* scenarios in the AMI can be characterised by a reduced upstream flow of usage data and downstream flow of service data. This could consequently lead to load estimation errors, bad pricing models, and reduced service quality for customers. Furthermore, as modelled in [23], the hierarchical structure of the AMI can cause a larger number of nodes lower down in the chain to lose connectivity to the core, further exasperating the issue.

Meanwhile, the Load Frequency Control sub-system may use SCADA protocols like ICCP (Inter Control Center Protocol) [12] or the IEC 61850 protocol stack [15] running on top of TCP/IP infrastructure [12] [7] to ensure RTU-to-core communication. Flooding-style attacks can therefore be deployed here too, as examined by [14]. *A.1* scenarios in the LFC system would be characterised by the untimely or reduced sharing of telemetry data by RTUs. This could result in incorrect control signal generation and consequently, the incorrect operation of physical grid devices, which may escalate into grid instability. Furthermore, it should be noted that ICCP and IEC 61850 do not provide robust and secure authentication mechanisms [12] [7], leaving these communications vulnerable to malicious influence. The mechanisms for how flooding may be achieved on channels using these protocols (and for DoS in general) is an area for further study.

The survey also threw up the threat of *A.1* scenarios against the Phasor Control sub-system, which may use IEC 61850 protocols too [15]. This attack possibility was explored by [25], where the authors examined the relationship between PMU data and control signals. The results of their experiments suggest that the prevention of timely measurement readings due to flooded communication channels can result in incorrect control signals, which in turn may lead to fluctuations in frequency and ultimately, an unstable grid. This assessment on the impact of disrupted PMU flows was also supported by the results of [21]. A similar angle may be considered for the Telemetry Control and Core Control sub-systems as well.

Saturation scenarios on TCP/IP connections may be dealt with using anomaly detection to identify increases in traffic volume. This is also applicable against low-rate DoS attacks [26]. Similarly, IDS (Intrusion Detection Systems) should be used to identify suspicious activity, including jamming attacks [5]. For external attack sources, traffic from suspected IPs can then be blocked. Both anomaly detection and IDS (Intrusion Detection Systems) should be deployed at each layer of the cyber hierarchy [8]. Honeypots are suggested by [23] and can absorb attack impact. Saturation attacks can also be prevented by minimising the number of device and server interfaces with remote access. For the disruption caused by ongoing DoS attacks, Li et al. [13] suggested the use of predictive algorithms and historical data to estimate correct values and maintain grid stability. Meanwhile, SCADA and other control layer protocols need to introduce stronger authentication and improved security.

4.2 Network Exploit Scenarios (*A.2*)

Wireless ad-hoc network architectures are designed to be self-forming so that nearby nodes can organise themselves to define routes for data transmission. As stated previously, mesh networks may be deployed in the AMI (and possibly within the wider distribution and transmission domains for field sensors). However, the protocols used may be exploited to prevent these networks from forming and/or stabilising. This possibility was explored by [27], who defined the puppet attack against the DSR protocol. Other ad-hoc routing protocols like RPL (Routing Protocol for Low-Power) or OLSR (Optimized Link State Routing) may also be vulnerable to similar attacks. The result of an *A.2* scenario in the AMI may therefore be characterised as a customer domain network which has failed to converge and so no smart meter data can be delivered. Jamming attacks can similarly disrupt the normal operation of wireless network protocols [5].

As suggested in [17], LTE-based cellular networks may be used as an AMI architecture. In this type of setup, bearers are created to link devices to the data network. Bearer assignment may be exploited in a method similar in concept to TCP SYN; channels are opened to the target and then not used. As a result legitimate access is denied [17]. Once again, this would lead to the denial of AMI services.

Another possible *A.2* scenario is the exploitation of AMI NAT systems, as identified by [17]. Despite the introduction of IPv6, IPv4 is still widely used. This means that NAT is required for both translating between private and public IPv4 addresses, and for IPv4-to-IPv6 mappings [17] [11]. For example, if field sensors using IPv6 attempt to send data to core networks still operating on IPv4, the corruption of NAT64 mappings would deny such transmissions. In cases such as this and in LTE networks, *A.2* scenarios will be characterised by a lack of connectivity between endpoints. We did not identify *A.2* scenarios for the other sub-systems during our survey and suggest this as an area for further study.

To avoid network disruption, routing protocols should be secure against tampering attempts, and robust enough to re-converge efficiently. Such an approach

was proposed by [21] whose topology configuration scheme is designed to maintain routing between PMUs and RNs. Similarly, [27] suggested that corrupted nodes be identified by their abnormal communications and isolated, given that WSN nodes depend on their neighbours for their network connectivity. For field networks, physical security is needed to prevent illegitimate devices from joining ad-hoc networks. Anomaly detection applied to network exploitation needs to monitor protocol activity rather than general communication traffic. For SMS links, [17] cited the use of machine learning with bearer-related data to achieve this. They also suggest that migrating more widely to IPv6 could reduce the need for NAT mappings, thus reducing the risk of this type of DoS [17].

4.3 Device Exhaustion Scenarios (*B.1*)

Certain devices may be specifically targeted. An example in the Phasor Control sub-system is the relay nodes between PMUs and control systems, as highlighted by [21]. Given the large number of data collection points, relay nodes are used to ensure end-to-end delivery, sometimes also acting as aggregators. A targeted DoS attack on these devices can therefore disrupt the whole sub-system's communication flows, again leading to inaccurate measurements being collected. Furthermore, it is plausible to assume that relay node services in other sub-systems, such as the AMI, Load Frequency Controls, and Telemetry Controls, can be denied in this way too.

PLCs (and their interfaces) may also be actively targeted, as highlighted by [28]. Like relay nodes, PLCs have a central role in data collection and aggregation, but are more closely integrated with core control systems. Therefore, deliberate disruption of PLCs will significantly impact management decisions. The same scenario may be applicable to RTUs too. However, devices such as these, which are found deeper within the smart grid architecture, should theoretically be more difficult to access and would require insider access or skilled adversaries. Therefore, *B.1* scenarios in such systems will be characterised by the likely presence of skilled attackers or malicious insiders, and the hindering of data delivery to the core.

Finally, direct attacks within the AMI may be directed at smart meters, overwhelming their processing capacity as demonstrated by [23] and [19]. Unlike attacks on the AMI channels, forcing smart meters offline has the benefit of preventing both their communications with appliances and with head nodes directing traffic to the core. The location of smart meters within customer premises also exposes them as easier targets. Furthermore, [23] and [19] both demonstrated that AMI aggregator nodes and utility servers can be directly targeted. Attacks may be in the form of TCP SYN flood, HTTP flood, or other similar device-focused TCP/IP methods. Therefore, these *B.1* scenarios will be characterised as disabled devices within the AMI tree, with diminished connectivity for all the nodes served by them.

B.1 is the device-focused equivalent of *A.1*, so similar defensive measures may be applied. The aim is to knock particular devices offline, so suspicious traffic directed at those devices can be identified using anomaly detection. Anomaly

profiles should be derived from the normal activity of those devices, with consideration of typical performance values, and critical nodes may be prioritised to reduce the overheads introduced by this. Predictive algorithms may again be applied to control systems to reduce the impact of lost telemetry data [13]. To deal with possible insider threats, [28] recommends strict monitoring and regulation of user privileges and activities.

4.4 Device Compromise Scenarios (*B.2*)

A possible compromise scenario is where smart grid devices are recruited into botnets. Whilst this is less probable in the deeper areas of the grid (given that those devices may be running proprietary software and may be difficult to physically access), it should not be completely disregarded as a possibility where malicious insiders are considered. Bot compromise is most likely to occur within edge systems (like the AMI), where some devices sit within customer premises and may be exposed to public networks. As highlighted in [8], a population of smart meters (with similar manufacturers and models) could see the spread of bot code via an automated malware. IoT-based botnets (made up of smart appliances) are also a factor. Whilst a botnet compromise is itself not necessarily a DoS scenario, it provides a platform from which to launch such attacks. Additionally, bots provide backdoor access and can serve as vectors for smaller and more targeted DoS campaigns. Botnet-based DDoS, where smart meters are compromised, was studied by [8], and similar botnet scenarios were considered by [23], [20] and [3].

Another *B.2* scenario, primarily targeting the field sensors, is the forced depletion of physical resources on the target device. This is especially problematic in low power networks such as those in WSNs. For example, the Denial-of-Sleep attack defined by [9] is designed to drain the energy of battery-powered sensors and control devices to render them non-functional. Whilst the impact of such an attack may be slower to manifest, it could have a longer-term impact on service quality as depleted nodes would need to be physically changed. The loss of nodes in the AMI would reduce its overall accuracy and functionality, but Denial-of-Sleep could plausibly be used against any type of battery-powered field device. *B.1* scenarios may therefore be characterised by the presence of grid devices over which the operators do not have full control.

To stop nodes from being recruited into a botnet, devices must be regularly updated and patched with the latest software to minimise vulnerabilities. This can be challenging for difficult-to-access field sensors with limited capacity, which highlights the need for security-by-design in such devices. Login credentials must also be properly configured, as default passwords can be used to gain access [2]. Battery depletion can be mitigated by designing more energy-efficient devices, and connecting nodes to the main power where possible. To deal with Denial-of-Sleep, [9] suggested the need for an additional security layer for key exchanges to prevent meters being forced into FAC (Frequent Access Cycle).

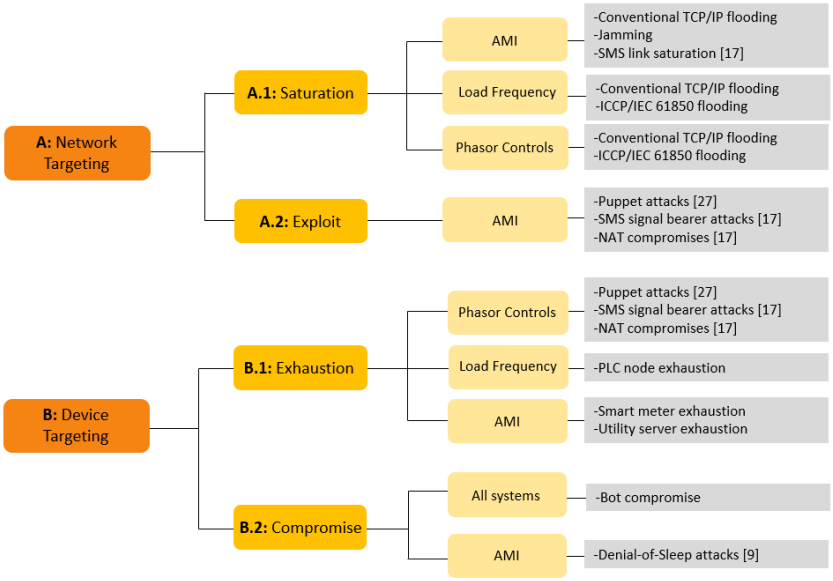

Fig. 3. Smart grid DoS attack classification tree.

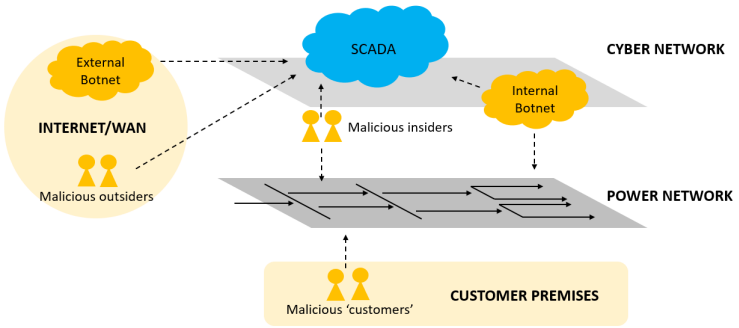

Fig. 4. Smart grid DoS attack sources.

Fig. 3 summarises and depicts the smart grid DoS scenario classifications described here, and Fig. 4 illustrates where DoS attacks sources may sit in relation to the smart grid.

5 Discussion

In this work, we sought to uncover where and how DoS attacks may manifest in the smart grid. Given that this is still a relatively new technology, there have thankfully been very few real-world attacks thus far, for which (to our

knowledge) detailed data is not available. Therefore, we turned to the available cyber-security literature and our understanding of smart grid architectures (combined with what we know of typical DoS attacks) for answers. We believe that this proved to be a sound methodology, as through the survey, we were able to enumerate and identify the sub-systems which could be targeted and how. This provides defenders with a means to prioritise their methods. It also provides future researchers with a reference point for what has been done so that other sub-systems may be considered as well. For example, areas for future DoS research may include attacks against generators and distributed power generation, and those originating from within the corporate networks of service provides or the Markets domain.

Through the survey, we were able to identify that the research community considers the AMI to be the most likely target of DoS attacks, with botnets being the most likely source. This suggests the need for better AMI security measures, and relates to other open research topics such as the security of IoT devices and WSNs. Meanwhile, the definitions of Denial-of-Sleep by [9] and puppet attacks by [27] demonstrate how the particularities of the smart grid can create space for new attack scenarios. Both scenarios were set in the AMI, once again highlighting the need for resilient security channels, as well as security-by-design in IoT technologies. It is also worth noting that these attacks may be feasible wherever mesh networks or battery-powered devices are used across the grid domains.

The potential vulnerability of other systems, despite their locations deeper within the grid network, is also apparent in the works of [25] and [21] who observed the impact of DoS on PMUs, and [28] and [14] who did the same for PLCs and LFCs, respectively. These components are likely harder to impact remotely and without specialist knowledge, but may still be targeted by skilled attackers (e.g. those working on behalf of nation states). The location of such components, higher up within the grid hierarchy, also means that the impact of any successful attack will be felt throughout the grid. Therefore, these systems must be secured appropriately.

Furthermore, we believe that the proposed classification provides a novel perspective for smart grid DoS. There are many classifications of DoS attacks in the existing literature, but most focus on the methodology. This is appropriate for the high-level characterisation of generic DoS attacks, but we argue that in the context of smart grids, it is beneficial to characterise attacks by target and impact, as this helps to align them with the IT and OT layers. Simply, this view enumerates the grid's vulnerable points. Furthermore, it makes a distinction between attacks against the channel and against the device. This is not always clear in exploit-based DoS scenarios, but is significant in smart grids because the domain of attack and the domain of impact can be different. By determining where an attack is intended to cause damage, we can work towards expanding typical DoS defence methods.

Due to scope restrictions, the survey itself was not exhaustive and can also be expanded - the smart grid is a complex web of sub-systems spanning the IT, OT, and domains. Therefore, another possibility for future work is to build

upon this survey to uncover more grid systems which may be vulnerable to DoS attacks, both known and novel. We assume that as smart grids become more well-established, the research into their security will also grow. Finally, as mentioned in Section 4.1, protocols developed for critical infrastructure may be further studied to uncover new DoS attack methods and possible exploits.

6 Related Work

The novelty of this work comes from our singular focus on DoS scenarios for smart grids, with special consideration for smart grid sub-systems, supported by a survey of the existing literature on the subject. Whilst there are many works considering the different types of DoS attack and the cyber-security challenges faced by smart grids, few works focus on both at the same time. In addition to this, most existing classification schemes deal with methodology whilst this work aims to highlight the relationship between attack targets and attack impact.

Huseinovic et al. [10] developed a taxonomy of possible DoS attacks based on available literature, followed by a discussion of defensive strategies. Similar to this work, they explored different taxonomy perspectives, including one that considers which grid applications are targeted. However, they put more emphasis on analysing the security measures against each attack type and did not provide in-depth characterisations as we have. Otuoze et al. [16] also considered an alternative classification perspective by looking at threat sources, identifying both technical (i.e. infrastructural, operational, data) and non-technical (environmental, policy) sources, but did not provide details on DoS scenarios.

Wang and Lu [24] contributed a thorough survey of cyber-security challenges in the smart grid, with a section dedicated to DoS threats. However, they did not examine different sub-systems to characterise and classify attacks as we have. El Mrabet et al. [6] conducted a similar survey but also did not offer characterisations. In their extensive cyber-security survey, Tan et al. [22] did consider different smart grid components, but organised them differently as sub-systems (AMI, SCADA/WAMS) and data-generating devices (smart meters, PMUs, etc). Meanwhile, they did not look in detail at DoS scenarios. Our work sits alongside this to provide an alternative perspective.

Lastly, Ramanauskaite and Cenys [18] created a detailed taxonomy of DoS attack types and the defences against them, including considerations of attack source, exploited vulnerabilities, method, target type, and rate. However, smart grids were not in the scope of their work and so they did not consider the grid-specific attack targets. As with [22], we believe our work sits alongside this to help focus in on smart grid-specific DoS threats.

7 Conclusions

Smart grids are designed to make the generation and provision of power services more efficient and sustainable through the integration of IT technologies. However, this exposes the OT to cyber threats as seen in conventional networks

and the Internet. DoS and DDoS attacks are among the most prevalent of these threats. This work provides a survey and a summary of the grid sub-systems that may be targeted, and characterises several possible DoS scenarios, alongside a target-based classification scheme to support this new perspective. Overall, we hope to have highlighted areas of smart grid vulnerability and set a foundation for better DoS defence and mitigation.

Acknowledgment

This work is funded by and a part of Energy Shield, a project under the European Union's H2020 Research and Innovation Programme.

References

1. Energy Shield (2019), https://energy-shield.eu/, last accessed 18th December 2019
2. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., et al.: Understanding the Mirai Botnet. In: 26th {USENIX} Security Symposium ({USENIX} Security 17). pp. 1093–1110 (2017)
3. Asri, S., Pranggono, B.: Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure. Wireless Personal Communications **83**(3), 2211–2223 (2015)
4. Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M.: Lessons from Applying the Systematic Literature Review Process Within the Software Engineering Domain. Journal of Systems and Software **80**(4), 571–583 (2007)
5. Chatfield, B., Haddad, R.J., Chen, L.: Low-Computational Complexity Intrusion Detection System for Jamming Attacks in Smart Grids. In: 2018 International Conference on Computing, Networking and Communications (ICNC). pp. 367–371. IEEE (2018)
6. El Mrabet, Z., Kaabouch, N., El Ghazi, H., El Ghazi, H.: Cyber-Security in Smart Grid: Survey and Challenges. Computers & Electrical Engineering **67**, 469–482 (2018)
7. Elgargouri, A., Virrankoski, R., Elmusrati, M.: IEC 61850 Based Smart Grid Security (03 2015). https://doi.org/10.1109/ICIT.2015.7125460
8. Guo, Y., Ten, C.W., Hu, S., Weaver, W.W.: Modeling Distributed Denial of Service Attack in Advanced Metering Infrastructure. In: 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). pp. 1–5. IEEE (2015)
9. Hoffmann, S., Bumiller, G.: Identification and Simulation of a Denial-of-Sleep Attack on Open Metering System. In: 2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe). pp. 1–5. IEEE (2019)
10. Huseinovic, A., Mrdovic, S., Bicakci, K., Uludag, S.: A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures. In: 2018 26th Telecommunications Forum (TELFOR). pp. 1–4. IEEE (2018)
11. IETF: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers (2011), https://tools.ietf.org/html/rfc6146, last accessed March 2020

12. Knapp, E.: Chapter 4 - Industrial Network Protocols. In: Knapp, E. (ed.) Industrial Network Security, pp. 55–87. Syngress, Boston (2011). https://doi.org/https://doi.org/10.1016/B978-1-59749-645-2.00004-5
13. Li, Y., Zhang, P., Ma, L.: Denial of Service Attack and Defense Method on Load Frequency Control System. Journal of the Franklin Institute **356**(15), 8625–8645 (2019)
14. Liu, S., Liu, X.P., El Saddik, A.: Denial-of-Service (DoS) Attacks on Load Frequency Control in Smart Grids. In: 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT). pp. 1–6. IEEE (2013)
15. Mattioli, R., Moulinos, K.: Communication Network Interdependencies in Smart Grids (2015), https://www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids, last accessed March 2020.
16. Otuoze, A.O., Mustafa, M.W., Larik, R.M.: Smart Grids Security Challenges: Classification by Sources of Threats. Journal of Electrical Systems and Information Technology **5**(3), 468–483 (2018)
17. Pedramnia, K., Rahmani, M.: Survey of DoS Attacks on LTE Infrastructure used in AMI System and Countermeasures. In: 2018 Smart Grid Conference (SGC). pp. 1–6. IEEE (2018)
18. Ramanauskaite, S., Cenys, A.: Taxonomy of DoS Attacks and their Countermeasures. Open Computer Science **1**(3), 355–366 (2011)
19. Sgouras, K.I., Birda, A.D., Labridis, D.P.: Cyber Attack Impact on Critical Smart Grid Infrastructures. In: ISGT 2014. pp. 1–5. IEEE (2014)
20. Sgouras, K.I., Kyriakidis, A.N., Labridis, D.P.: Short-Term Risk Assessment of Botnet Attacks on Advanced Metering Infrastructure. IET Cyber-Physical Systems: Theory & Applications **2**(3), 143–151 (2017)
21. Srikantha, P., Kundur, D.: Denial of Service Attacks and Mitigation for Stability in Cyber-Enabled Power Grid. In: 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). pp. 1–5. IEEE (2015)
22. Tan, S., De, D., Song, W.Z., Yang, J., Das, S.K.: Survey of Security Advances in Smart Grid: A Data Driven Approach. IEEE Communications Surveys & Tutorials **19**(1), 397–422 (2017)
23. Wang, K., Du, M., Maharjan, S., Sun, Y.: Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid. IEEE Transactions on Smart Grid **8**(5), 2474–2482 (2017)
24. Wang, W., Lu, Z.: Cyber Security in the Smart Grid: Survey and Challenges. Computer Networks **57**(5), 1344–1371 (2013)
25. Wei, J., Kundur, D.: A Flocking-Based Model for DoS-Resilient Communication Routing in Smart Grid. In: 2012 IEEE Global Communications Conference (GLOBECOM). pp. 3519–3524. IEEE (2012)
26. Xiang, Y., Li, K., Zhou, W.: Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics. IEEE transactions on information forensics and security **6**(2), 426–437 (2011)
27. Yi, P., Zhu, T., Zhang, Q., Wu, Y., Pan, L.: Puppet Attack: A Denial of Service Attack in Advanced Metering Infrastructure Network. Journal of Network and Computer Applications **59**, 325–332 (2016)
28. Yilmaz, E.N., Ciylan, B., Gönen, S., Sindiren, E., Karacayılmaz, G.: Cyber Security in Industrial Control Systems: Analysis of DoS Attacks Against PLCs and the Insider Effect. In: 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG). pp. 81–85. IEEE (2018)