Modelling DoS Attacks & Interoperability in the Smart Grid

Dilara Acarali, Muttukrishnan Rajarajan
School of Mathematics, Computer Science & Engineering
City, University of London
London, UK
{dilara.acarali, r.muttukrishnan}@city.ac.uk

Doron Chema, Mark Ginzburg
Technical Team
L7 Defense
BeerSheva, Israel
{doron, marik}@l7defense.com

***Abstract*—Smart grids perform the crucial role of delivering electricity to millions of people and driving today's industries. However, the integration of physical operational technology (OT) with IT systems introduces many security challenges. Denial-of-Service (DoS) is a well-known IT attack with a large potential for damage within the smart grid. Whilst DoS is relatively well-understood in IT networks, the unique characteristics and requirements of smart grids bring up new challenges. In this paper, we examine this relationship and propose the OT impact chain to capture possible sequences of events resulting from an IT-side DoS attack. We then apply epidemic principles to explore the same dynamics using the proposed *S-A-C* model.**

***Index Terms*—Smart grids, cyber-security, DoS, DDoS**

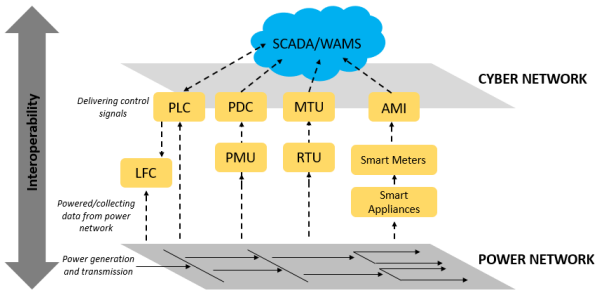

Fig. 1. Smart grid IT and OT interoperability.

I. Introduction

A smart grid is the modern manifestation of the traditional power grid. The 'smart' label denotes the addition of communication devices for real-time monitoring and response. A communication network (the IT or Information Technology) is overlaid on top of the existing physical power network (the OT or Operational Technology). The smart grid therefore consists of two distinct but inter-connected, interdependent networks [1]. The IT remotely connects control systems to devices in the field that collect data. Based on this data, control systems issue control commands to alter topology, change settings, adjust loads, and recover from faults.

However, remote connectivity can also be a vector for malicious activity. Communication channels are integrated throughout the grid, exposing areas that were previously difficult to compromise. A possible compromise scenario is Denial-of-Service (DoS) [2], where attackers aim to prevent systems performing their normal operations. DoS or DDoS (Distributed DoS) can block communication flows in the smart grid, disrupting monitoring and management. This can ultimately lead to instability and outages.

Conventional TCP/IP networks are complex systems of systems. This presents a myriad of security issues. The smart grid's cyber network is similar, but it is also intertwined with an underlying physical network responsible for the generation and provision of energy. The criticality of this service increases the risk of and fallout from attacks. The two networks (Fig. 1) are both interdependent (i.e. they depend on each other for functionality) and interoperable (i.e. many grid processes run on both simultaneously). Hence, the IT-OT relationship is vitally important when designing security solutions.

However, the security implications of this relationship are not well-understood. DoS remains a relatively easy yet effective attack. Whilst this attack is well-studied in conventional networks, there is less research for DoS in the smart grid. The IT-OT relationship, service criticality, and strict performance requirements of the smart grid set it apart and must be addressed to pre-emptively mitigate the DoS threat. In this work, we address this by considering how DoS attacks originating in different areas of the IT may affect the OT. We examine the IT-OT relationship and propose the OT impact chain to qualitatively capture the sequence of escalating impact events that may be caused within the OT. We also propose the epidemiological *S-A-C* model to support the impact chain with quantitative analysis. To our knowledge, epidemic modelling has not been used in this context before.

The core contributions of this paper are:

- The new OT impact chain framework to capture DoS attack characteristics for qualitative assessment of possible effect chains, based on grid system relationships.
- The novel use of epidemic modelling with the *S-A-C* model to qualitatively predict DoS impact scale, based on the IT-OT dependency.

In recognition of the proliferation of smart grids and the threat posed by DoS attacks, the European Union has initiated the Energy Shield project [3] for the development of appropriate defences. The work presented in this paper was conducted as part of this project, with the goal of applying

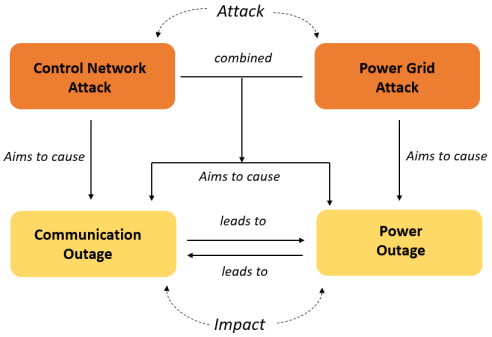

Fig. 2. Smart grid cascading attack process.

existing modelling techniques to DDoS in novel ways in order to improve smart grid defences.

Section II outlines interoperability, inter-dependency, and cascading failures, followed by a formal description of the OT impact chain framework. Section III provides a definition of the *S-A-C* epidemic model and the findings of some early numerical simulations to test parameters. In Section IV, we discuss the implications of the two contributions and their use, and related work is presented in Section V. We then conclude in Section VI.

II. Smart Grid DoS & OT Impact Chain

A. Interoperability & Cascading Failures

The integration of the IT and OT results in interoperability requirements. Interoperability is where two or more systems "exchange information and use the information that has been exchanged" [1]. For this to work, systems must operate to a common standard, defined by the data structures, protocols, and communication channels used. This relates to domain interdependency because the management of OT devices depends on accurate and timely data flows through the IT. Therefore, an IT failure can have a cascading affect on the rest of the grid.

A cascading failure propagates from a point throughout an interconnected system, such that it impacts more and more of that system. Two types of cascading failure in smart grids are 1). where an overloaded line fails and trips, and its load is redistributed amongst neighbouring lines which may then also become overloaded, and 2). where an IT issue disrupts the flow of sensor data and control signals, causing OT mismanagement. If parts of the OT then fail, this exasperates issues in the IT (e.g. communication devices may go offline). Hence, failures 'cascade' both within and across the networks. Fig. 2 illustrates this concept. We focus on attacks against the IT (i.e. communication flows), which have subsequent impact on the OT, since we consider this to be the more likely compromise scenario.

B. OT Impact Chain Definition

The OT impact chain is designed to capture the relationship of IT-side DoS attacks and the proliferating OT-side impact they can have. It provides a means for the qualitative assessment of DoS attacks, such that the initial, secondary, and continuing impact of the attack, depending on where it lands in the IT network, can be considered. The main fields to be defined in the framework are:

- **Attackers:** Devices that transmit DoS attack packets.
- **Attack Point:** IT systems targeted in the DoS attack.
- **DoS Attack:** DoS attack itself, including:
  - *DoS Type:* Flood attack, protocol compromise, etc.
  - *Attack Rate:* Inter-arrival time for attack packets.
  - *Compromise Probability:* Likelihood of target service loss.
- **Initial IT Impact:** Initial impact (devices affected, how many) on IT systems local to DoS targets.
- **Initial OT Impact:** Initial impact of compromised IT systems on directly connected OT systems.
- **Consequent Impact:** Rounds of impact in the OT, caused by compromise of OT systems in previous impact rounds.
- **Intra-IT Interoperability:** Assessment of intra-IT connectivity and dependency relationships.
- **Intra-OT Interoperability:** Assessment of intra-OT connectivity and dependency relationships.
- **Inter-IT-OT Interoperability:** Assessment of IT-OT connectivity and dependency relationships.

Fig. 3 shows the basic framework structure. The attack source may be internal but is more likely to be external. It is also likely to be a botnet [4]. The DoS attack lands in the IT, compromising a specific target (e.g. a channel or a device). Attack potency will depend on packet rate and the number of attackers. If successful, the attack has initial local IT impact i.e. IT nodes dependent on the target will be affected. Local impact will depend on the degree of intra-IT interoperability, which is defined by a qualitative assessment of IT systems and the dependencies between them.

Inter IT-OT interoperability is similarly defined. Depending on the IT attack site, there will be a direct impact on OT devices that are connected to the IT target. This is the initial OT impact. Intra-OT interoperability then determines how dependent OT systems are on each other. Given that OT systems stabilise the grid, a compromise can escalate, as captured by the rounds of consequent impact (2nd, 3rd, and so on). Hence, the compromise spreads throughout the grid as wider grid functions are affected by the loss of singular functions or processes. Nodes in each impact step are affected by the compromised nodes of the previous step. The speed of this will vary with each scenario.

DoS attacks may block sensor data from reaching the control centre, preventing timely and accurate control signals being generated. If the correct adjustments are not made to grid devices, failures may result. DoS may also use crafted packets to manipulate OT system operations to cause device failures [5]. Fig. 4 shows some possible scenarios against the channels or devices of different grid sub-systems. For example, AMI attacks can cause channel saturation or server failure. Exploitation of network protocols can cause network

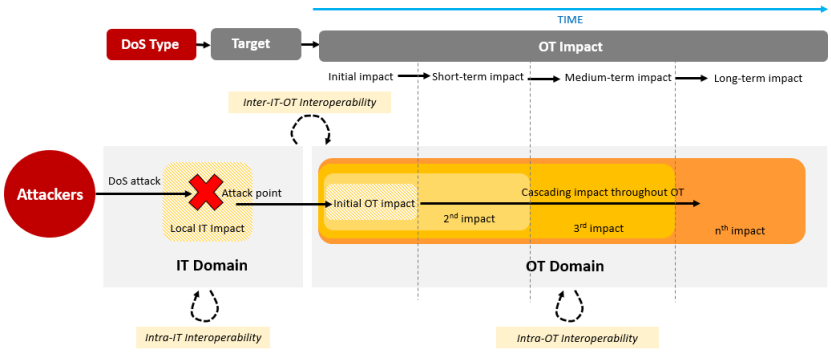

Fig. 3. Definition of OT impact chain.

instability. This could lead to load forecasting errors as data sharing is blocked, which may cause load instability, triggering line failures or load shedding. The hierarchical nature of both the IT and OT is reflected in the impact chain, which has a tree-like structure. This demonstrates the relationships between attack targets and impact areas, and between small-scale and large-scale compromises as incidents develop over time.

III. Smart Grid DoS & Compromise Epidemic Model

A. S-A-C Epidemic Model Definition

To quantitatively support the OT impact chain, we developed the *S-A-C* (Susceptible, Attack, Compromised) epidemic model, depicted in Fig. 5. This is a work-in-progress, and in its current state, is a deterministic model to capture a high-level view of the events discussed in Section II. Specifically, it explores the influence that compromised IT systems have on both the IT and the OT. Based on epidemiological concepts, a population of devices is split into sub-populations, each representing a possible state. A series of differential equations then define the rates of change of sub-population sizes as devices (AKA nodes) move between states.

The parameters are summarised in Table 1. The model consists of two separate network populations, c (cyber) and p (physical), which are each split into susceptible (S) and compromised (C) states. A separate population of attacking nodes (A) exists, representing an external DDoS-enabled botnet. In c, the number of compromised nodes depends on the number of A nodes, the attack rate β, and contact between A and S_c nodes, as well as contact between S_c nodes and existing C_c nodes. In p, the size of the C_p population depends on the contact between S_p nodes and compromised C_c nodes in the IT, as well as the contact between S_p and existing C_p nodes. In both networks, compromised nodes recover at the rate α, defaulting back to the S state.

The attack rate β abstractly represents the force of the DDoS campaign and subsumes attack packet delivery rate and the probability of compromise success. It is defined as the product of DoS packet size m_{DoS}, DoS packet arrival rate a_{DoS}, and the probability of disruption for arriving packets p_{DoS}. The recovery rate α is set manually to denote the level of defender response. Meanwhile, we define ω_c as a figure which

Parameter	Definition
c	Cyber (IT) population
p	Physical (OT) population
S	Susceptible; nodes vulnerable to compromise.
A	Attackers; nodes engaged in the DoS attack.
C	Compromised; nodes affected by the DoS attack.
S_c	Susceptible nodes in the IT population.
C_c	Compromised nodes in the IT population.
S_p	Susceptible nodes in the OT population.
C_p	Compromised nodes in the OT population.
β	DDoS attack rate.
α	Recovery rate for compromised nodes.
ω_c	Interoperability coefficient within the IT network.
ω_p	Interoperability coefficient within the OT network.
ω_{cp}	Interoperability coefficient between IT and OT networks.
m_{DoS}	Mean size of DoS attack packets.
a_{DoS}	Mean arrival rate of DoS attack packets.
p_{DoS}	Delivery and success probability of DoS attack packets.

TABLE I
S-A-C MODEL PARAMETER DEFINITIONS.

denotes the average degree of node interoperability or interdependency within the c population. Similarly, ω_p represents the same for the p population, and ω_{cp} represents average interoperability between c and p nodes.

Unlike standard epidemic models, the A population remains constant, allowing us to control the number of DDoS participants in each run. To keep the process simple, we also assume homogenous mixing within and between the two networks. The transitions are defined mathematically as follows:

$$S_c dt = -(\beta S_c A) - (S_c C_c \omega_c) + (\alpha C_c) \quad (1)$$

$$C_c dt = (\beta S_c A) + (S_c C_c \omega_c) - (\alpha C_c) \quad (2)$$

$$S_p dt = -(S_p C_c \omega_{cp}) - (S_p C_p \omega_p) + (\alpha C_p) \quad (3)$$

$$C_p dt = (S_p C_c \omega_{cp}) + (S_p C_p \omega_p) - (\alpha C_p) \quad (4)$$

$$A dt = 0 \quad (5)$$

B. OT Impact Model Findings

To explore how population dynamics are influenced by the *S-A-C* parameters, we manually performed preliminary numerical simulations by testing a range of values for each parameter and comparing to a baseline. In this baseline, we define a starting population of 1000 nodes each for c and

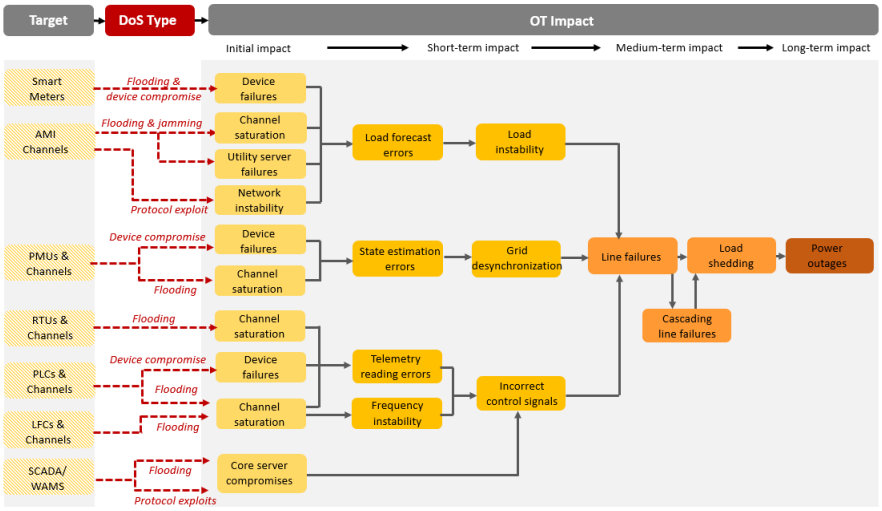

Fig. 4. Smart grid DoS attack targets and possible impact events.

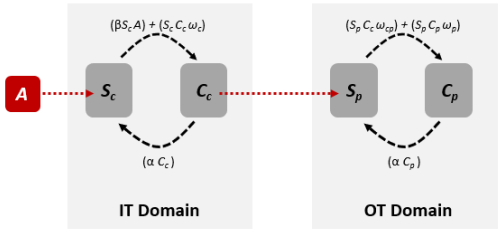

Fig. 5. *S-A-C* model states and transitions.

p, emulating a grid sub-system which has both IT and OT components. We also set a minimum botnet population A of 50 nodes, which is then increased over subsequent tests. Baseline interoperability values for ω_c, ω_p, and ω_{cp} were all set to 0.5 (where 0 would denote none, and 1 would denote full dependency). The basic dynamics of the model are as follows. As S_c declines, this deficit is absorbed directly into C_c so that on a graph, the two curves mirror each other, as shown in Fig. 6. The same applies to the relationship between S_p and C_p. Compared at higher attack rates, the decline in S_p has a less steep slope and lower minimum value because attacks drive compromises up in c directly. However, if β is minimised, peak C_p is higher, as fewer new compromises take place within c but existing C_c nodes are enough to continue causing compromises within p.

As per intuition, minimising α causes a larger number of compromises overall. As α is increased, the downward slope of both S populations becomes less steep, and the gap between the peak final S_c and S_p populations narrows significantly. This is because there are fewer C_c nodes to drive compromises within p. Similar effects in the respective networks can be seen when ω_c and ω_p are manipulated, and when the A population is increased.

When m_{DoS} is very low (e.g. 1MB), there are more C_p nodes than C_c. This is because the attack rate β is driven down, so fewer compromises occur in c. As m_{DoS} increases, the peak value of C_c pushes up passed that of C_p. The greatest increase in IT compromises happens when the value of p_{DoS} approaches 1. When p_{DoS}=1, every single packet lands a successful hit on the target, maximising the efficiency of the attack. Hence, mitigating the arrival and affect of incoming packets can be an effective defence. Fig. 7 and 8 demonstrate the effects of increasing ω_p and ω_{cp}. Here, p's relationship to c has an effect similar in magnitude and severity to that of the internal characteristics of p. The notable difference is that increases in ω_{cp} result in more gradual increases, which can be explained by the delay between the initial compromise of c nodes and the impact being felt amongst p nodes.

When exploring ω values, we introduced an experimental definition of interoperability to further detail c-p connectivity. If we observe not the whole grid, but a particular sub-system, ω_{cp} is calculated as the product of mean sub-system node degree, mean contact rate within that population, and the criticality coefficient λ_c for the IT part of the sub-system for attached OT devices. Hence, the weighting applied to IT-OT dependency is a function of how critical IT and OT components are to each other. Early testing showed that increases in mean degree and λ_c have more chance of causing full scale OT compromise, and are far more influential on the OT than other parameters. Overall, this preliminary work shows that the model is a feasible approach. Further development and simulations, including a definition of λ_c, are planned.

IV. Discussion

The OT impact chain enables the characterisation of the relationship between the IT and the OT in several ways. Firstly, it encourages users to consider which part of the IT a cyber-attack is targeting. This directly influences the types of problems that will result in the OT. Secondly, it encourages defenders to consider what effect the loss or disruption of a particular sub-system may have on the wider

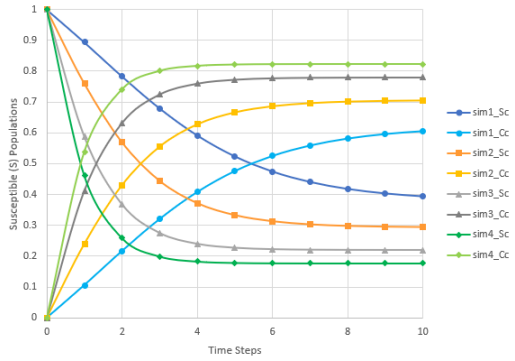

Fig. 6. Changes in S_c and C_c for β={0.1, 0.25, 0.5, 0.75}.

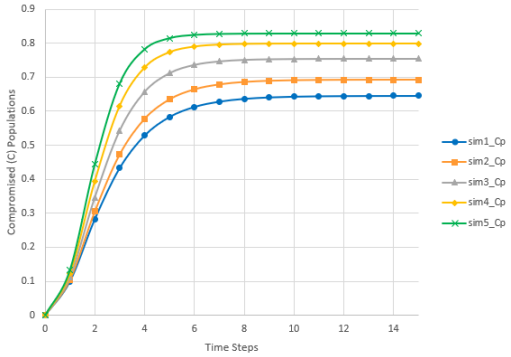

Fig. 7. Changes in C_p for ω_p={0.1, 0.25, 0.5, 0.75, 0.99}.

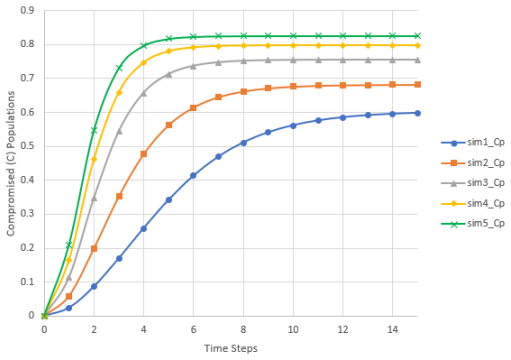

Fig. 8. Changes in C_p for ω_{cp}={0.1, 0.25, 0.5, 0.75, 0.99}.

grid via a qualitative assessment of the IT, OT, and IT-to-OT interdependencies. By mapping the relationships between sub-systems, we can better predict impact propagation scenarios, and by considering the worst case scenarios (i.e. blackouts), the appropriate preventative measures can be taken. Given the current threat landscape, we believe it is plausible to assume that attackers who decide to target the smart grid will do so with the intention of causing as much damage as possible.

The current OT impact chain was the result of our studies into smart grid DoS attacks. Given its focus on the relationships between grid sub-systems, we believe that it can be applied to other types of attack too. The main limitation of the current impact chain is that it does not consider the effect of OT-side failures (caused by the initial DoS) on the IT network. This could be achieved by expanding the fields already defined in the Section II.B. For example, interoperability will need to be assessed in terms of whether IT or OT devices drive a given process, so that there are separate definitions for IT-to-OT and OT-to-IT relationships. This is an area to be developed in future versions of the framework. In addition to this, we would like to develop a detailed characterisation of interoperability relationships between common smart grid sub-systems, which can be added to the framework as a baseline reference for users.

Epidemic modelling is typically used to trace the spread of infectious malware in IT networks by tracking the number of network nodes occupying different states over time. This quantifies the ongoing impact of a propagating issue. Thanks to this characteristic, the *S-A-C* model provides a quantitative assessment of the propagation of compromise, based on the relationships between nodes. This is a novel application of epidemiology (to our knowledge) and the results of preliminary testing presented in Section II.B demonstrate that this strategy has potential to uncover relationships between the modelled parameters. The planned future work is to develop this model further to add more complexity in line with the aforementioned characterisation of interoperability.

The main shortcoming of the *S-A-C* model is the assumption of homogenous mixing within and between populations. Whilst this provides a sufficient baseline understanding of the relationships between key model parameters, it may be considered unrealistic as communication and dependency between systems will depend heavily on the services they provide. Options to improve this include a sub-division of the overall c and p populations by grid sub-systems as defined in [6], or the use of dual directed graphs with cross-graph connectivity as defined in [7]. Such expansions would make *S-A-C* more applicable to both individual sub-systems and to the grid as a whole. Added complexity should be moderate, however, to ensure that the model remains easy to use. Finally, we would like to expand simulations to include more scenarios, and to use network (e.g. `ns-3` [8]) and power system (e.g. `GridLab-D` [9]) simulation environments to generate realistic data to further test and refine both the impact chain and the *S-A-C* model.

V. Related Work

In existing literature, interdependency is often approached using graphs, as introduced by Kundur et al. [7] who created an "impact analysis framework" using directed graphs to model the IT and OT as a pair of directed graphs, mathematically defining the impact relationships between them. They showed that systems and behaviours can be accurately represented, but did not explicitly consider security or attack scenarios. Inspired by [7], Yang et al. [10] created a graph-based simulation model of delays and malicious signals. Similar to us, they considered attack impact (reporting topological errors and generator overload), but for FDI (False Data Injection) rather than DDoS.

Similarly, Huang et al. [11] proposed a graph-based IT-OT interdependence model for the cost of maintaining the grid. Like us, they focused on cascading failures, mathematically defined as removals and fragmentations. They identified a threshold for the maximum number of faulty nodes permitted, but their failure simulations are generic and not based on particular attack scenarios.

Graph techniques are applied in recent works too. Wang et al. [12] used graphs to explore cascading failures caused by virus propagation, where the virus blocks communications. Classic epidemic models were used to represent the viral spread, and failure chains analysed. They demonstrated the role played by topology. The virus's malicious activities were not explicitly explored though. Gao et al. [13] proposed a stochastic model of cascading failures for vulnerability uncertainty. They integrated heterogeneity by considering node categories, and explored failures originating in the IT and OT. Their results suggested that high loads and load uncertainty made cascading failures worse. As with the other works, their failure trigger states are generic and they do not consider particular cyber-attacks.

Epidemiological principles are widely applied in different networks (e.g. WSNs [14], VANETs [15], and cloud [16]). Such techniques are now being applied in smart grid-related areas too. To study malware propagation, Shen et al. [17] developed the *V-C-Q-P-S* (Vulnerable, Compromised, Quarantined, Patched, Scrapped) model for sensor networks with heterogenous mobile nodes, extending the classic *S-I-R*. Simulation results showed that *V-C-Q-P-S* produces more accurate results, but interdependence was not considered. In contrast, Jiang et al. [18] focused specifically on propagation in interdependent networks, again based on the *S-I-R* model. Like us, their model considers a failure state partly triggered by failures of dependent nodes. The results suggest that interdependent networks are more vulnerable to epidemics. The particularities of smart grids are not considered.

Graph-based methodologies enable detailed analysis, but remain generic and can be highly complex. Meanwhile, use of epidemic modelling is still limited to generic networks or classic examples of malware propagation. Our aim is to take a focused approach to smart grid DDoS scenarios, and to provide a simple epidemiological approach to assess and predict the scale of impact. Unlike [12], [13], and [18], we couple our model with the impact chain to measure scale but also to characterise events. This is a novel approach, complementing both conventional DoS research and smart grid security research.

VI. Conclusions

Smart grids are a response to increased demand and the need for better efficiency. Modern IT systems connect grid systems to remote control centers, which has the unfortunate side-effect of exposing the grid to DDoS attacks. Interdependency and interoperability between the IT and OT can amplify the effect of such attacks. We have proposed the OT impact chain framework to help to characterise the short- to long-term impact of attacks landing within the IT. This is designed to enable a qualitative assessment of possible impact scenarios, based on the inter-connectivity of the grid. We then proposed the *S-A-C* epidemic model to add quantitative support to that assessment, capturing the scale of node compromise. This contributes to ongoing research into smart grid defence.

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] J. A. Momoh, *Smart Grid: Fundamentals of Design and Analysis*. John Wiley & Sons, 2012, vol. 63.

[2] NIST, "Guidelines for Smart Grid Cybersecurity," 2018, last accessed April 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[3] "Energy Shield," 2019, last accessed March 2020. [Online]. Available: https://energy-shield.eu/

[4] A. Wang, W. Chang, S. Chen, and A. Mohaisen, "Delving into Internet DDoS Attacks by Botnets: Characterization and Analysis," *IEEE/ACM Transactions on Networking*, vol. 26, no. 6, pp. 2843–2855, 2018.

[5] D. Upadhyay and S. Sampalli, "SCADA (Supervisory Control and Data Acquisition) Systems: Vulnerability Assessment and Security Recommendations," *Computers & Security*, vol. 89, p. 101666, 2020.

[6] D. Acarali, M. Rajarajan, and N. Komninos, "Modelling Botnet Propagation in Networks with Layered Defences," in *2018 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2018, pp. 1–6.

[7] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards Modelling the Impact of Cyber Attacks on a Smart Grid," *International Journal of Security and Networks*, vol. 6, no. 1, pp. 2–13, 2011.

[8] "ns-3 Network Simulator," 2020, last accessed March 2020. [Online]. Available: https://www.nsnam.org/

[9] "GridLab-D," 2019, last accessed March 2020. [Online]. Available: https://www.gridlabd.org/

[10] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. Wang, "Impact of Cyber-Security Issues on Smart Grid," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*. IEEE, 2011, pp. 1–7.

[11] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Balancing System Survivability and Cost of Smart Grid via Modeling Cascading Failures," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 45–56, 2013.

[12] T. Wang, X. Wei, T. Huang, J. Wang, L. Valencia-Cabrera, Z. Fan, and M. J. Pérez-Jiménez, "Cascading Failures Analysis Considering Extreme Virus Propagation of Cyber-Physical Systems in Smart Grids," *Complexity*, vol. 2019, 2019.

[13] X. Gao, M. Peng, K. T. Chi, and H. Zhang, "A Stochastic Model of Cascading Failure Dynamics in Cyber-Physical Power Systems," *IEEE Systems Journal*, 2020.

[14] S. Shen, H. Zhou, S. Feng, J. Liu, and Q. Cao, "SNIRD: Disclosing Rules of Malware Spread in Heterogeneous Wireless Sensor Networks," *IEEE Access*, vol. 7, pp. 92 881–92 892, 2019.

[15] P. Spadaccino, P. Conti, E. Boninsegna, F. Cuomo, and A. Baiocchi, "EPIC: An Epidemic Based Dissemination Algorithm for VANETs," in *Proceedings of the 1st ACM MobiHoc Workshop on Technologies, mOdels, and Protocols for Cooperative Connected Cars*, 2019, pp. 1–6.

[16] C. Gan, Q. Feng, X. Zhang, Z. Zhang, and Q. Zhu, "Dynamical Propagation Model of Malware for Cloud Computing Security," *IEEE Access*, vol. 8, pp. 20 325–20 333, 2020.

[17] S. Shen, H. Zhou, S. Feng, J. Liu, H. Zhang, and Q. Cao, "An Epidemiology-Based Model for Disclosing Dynamics of Malware Propagation in Heterogeneous and Mobile WSNs," *IEEE Access*, vol. 8, pp. 43 876–43 887, 2020.

[18] L. Jiang, Q. Xu, B. Ouyang, Y. Lang, Y. Dai, and J. Tong, "Epidemic Spreading in Interdependent Networks," *Mathematical Problems in Engineering*, vol. 2018, 2018.