Agent Based Simulation of Botnet Volumetric and Amplification Attack Scenarios Applied to Smart Grid Systems

Agent Based Simulation of Botnet Volumetric and Amplification Attack Scenarios Applied to Smart Grid Systems

[1]Callaghan Ebojoh
School of Computing and Eng
University of West London
United Kingdom
21502335@student.uwl.ac.uk

[1]Abel Yeboah-Ofori
School of Computing and Eng
University of West London
United Kingdom
abel.yeboah-ofori@uwl.ac.uk

Abstract--All industries rely on smart grid infrastructures and systems to energy systems to provide power supply to industries and individual users for innovation, economic growth and sustainability as part of SGD goals. However, recent attacks on the smart grid using various attack methods have made it inevitable to provide security implementation for sustainable development infrastructures and economic growth. Agent-based simulation (ABS) considers modelling complex adaptive systems in a heterogeneous environment to detect their interactive behaviours and attacks. Agents can represent people, households, and business entities in a smart grid system. ABSs are created with three core attributes, the declaration of the agent's architectures and associated agent classes, an agent environment, and the software modules to establish communication protocols between agents. However, threat actors can use these attributes to cause Distributed Denial of Service (DDoS) and False Data Injection Attacks (FDIA) on the smart grid. The paper presents an agent-based simulation of offensive botnet interactions within a smart grid system and considers amplification attack scenarios of DDoS and FDIA on the smart grid. The contribution of the paper is threefold. First, we explore how botnet agent attacks systems using ABS impact of cooperative defence during DDoS and FDIA attacks. Secondly, we implement attack models using GAMA tool to determine offensive botnet interactions within a smart grid system. Finally, we recommend control mechanisms to prevent offensive botnets on the smart grid network. The results show that ABS could be used to detect offensive botnet interactions within smart grid systems to improve cybersecurity.

Keywords: Agent-based Simulation, Botnet Agents, Distributed Denial of Service, False Data injection Attacks, Smart Grid, Cyber Security

I. INTRODUCTION

Agent-Based Simulation (ABS) modelling describes the simulation of complex adaptive systems focused on local emergence and heterogeneity in systems [1]. Smart grid infrastructure security has become inevitable since all economies, industries, societies and technologies depend on electric power efficiency for innovation, efficient business processes and socio-economic development and environmental sustainability. Recent attacks on the Ukrainian power plant attack to cut off power for about a day, the US Pacific North West power station attack that cut off 40,000 households and the Saudi Aramco power plant attack [22] shows that implementing botnet attacks on Smart grid could enhance infrastructure security and environmental security to improve SDG goals 8 and 9 that harnesses harness technological and infrastructural developments toward the 17 UN-defined SDGs.

The application of ABS considers the simulation of various complex systems, such as population dynamics [2], threat simulation of cyber-warfare between malefactors and security agents [20], and simulation of cooperation defence mechanisms against botnets [12]. Threat actors could penetrate smart grid and exploit the agent to create false narratives and data theft. The flexibility of ABS enables the development of emergent cyber threat phenomena that can be observed from local individuals' interactions. Agents can represent people, households, and business entities. ABSs are created with two core attributes. Agent-Based Simulation (ABS) modelling describes a set of experiments involving botmaster agents and how it deploy bots in the networks to cause FDIA and DDoS attack modelling and how the other agents react to that and the results of the defence mechanisms.

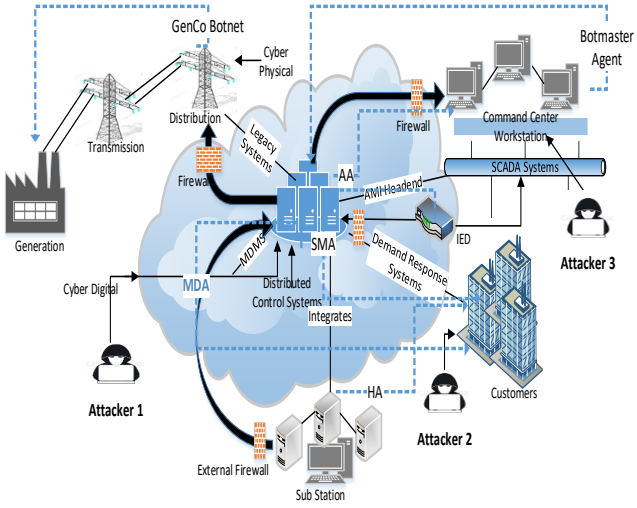

Fig 1. Botnet Attacks Agents on Smart Grid

Figure 1 presents how the botmaster agents interact with the various cyber digital components including the SCADA [22], and the cyber physical, cyber digital and human elements to communicate with the power plants generation and distribution systems [24]. The threat actor could penetrate the network, take command and control of the system and infiltrate, manipulate, exfiltrate and obfuscate leading to FDIA and DDoS attacks

An agent seeks an action, and tasks and has the ability to perform planning activities for future action. Belief-desire-intention model (BDI) is a decision framework that enables agents to switch plans dynamically based on internal beliefs.[3][4]. Traditional methods often fail to capture the complexity and evolution of a system dynamics such as an electricity market (EM). Closely coupled with an electricity market is the smart grid that deals explicitly with energy generation and energy transmission [3]. Due to the emergence of new technologies such as smart metering systems and variable generation systems, they can be integrated as inputs into the power grid. The smart grid intends to transform how energy is generated and decrease inefficiency in power transmission [5]. We explore volumetric scenarios in relation to cyber-attacks and their effect on smart grid infrastructure.

A. Security Challenges – Smart Grid Systems

This section discusses the various types of security challenges and attack patterns that threat actors can deploy to disrupt the operational activity of smart grid systems (SGS). SGS are electricity networks supported by digital communications technology and customer demand feedback that allow SGS to react to changes in demand to create more optimal electricity generation. The effects of small changes in smart grids from a normal operation can have adverse consequences for many consumers. Wadhawan et al. discuss the impact of blackouts, such as the Ukraine power grid attack, which led to power outages in thousands of households [7]. From a power generation supply side, power system infrastructure is designed to be fault tolerant. However, understanding the point of failure is often complicated due to the complexities of complex operationalising systems. From an adversary's perspective targeting smart grids can have financial rewards. Fadi Aloul et al. discussed the variety of attack patterns that are able to compromise SGS operations and deviate from a normal day of operation. [8] . We briefly discuss some of the challenges that impact the Smart Grid as follows:

- False Data Injection Attack (FDIA): Another cyber-attack pattern that can be used simultaneously and has similar effects to smart grid monitoring is FDIA. [9] Attackers can compromise the smart meter to report any false data collection activities resulting in a financial loss for the service provider.
- Blackout Outages: Cyberattack patterns that affect the source of power generation pose a severe risk to the energy supply causing significant disruptions such as the Ukraine power grid attack.
- DDoS Flooding: Flooding attacks are availability attack that is volumetric-based by maliciously creating DDoS attack by sending multiple requests through HTTP to the targeted recipient [10].

Threat actors can use these attributes to cause Distributed Denial of Service (DDoS) and False Data Injection Attacks (FDIA) on the smart grid. The paper presents an agent-based simulation of offensive botnet interactions within a smart grid system and considers amplification attack scenarios of DDoS and FDIA on the smart grid. The contribution of the paper is threefold. First, we explore how botnet agent attacks systems using ABS impact on cooperative defence during DDoS and FDIA attacks. Secondly, we implement attack models using GAMA tool to determine offensive botnet interactions within a smart grid system. Finally, we recommend control mechanisms to prevent offensive botnets on the smart grid network. The results show that ABS could be used to detect offensive botnet interactions within smart grid systems to improve cybersecurity.

II. RELATED WORKS

This section explores the start of the art and related works in agent-based simulation, botnet attacks Regarding ABM, Akhatova et al., (2022) proposed a Systematic Literature Review on ABS of urban district energy system decarbonization to address issues of complex and versatile methodologies in fostering transactions such as technologies, policies, processes and the roles of stakeholders, The authors used SLR and peer-reviewed analysis process to identify gaps in the application of ABS modelling. The results revealed existing gaps that focus on Innovation diffusion and dissemination of energy-saving behaviours [25]. Sriram et al., (2020) implemented a network-based IoT Botnet attack detection using Deep learning to enhance the quality of daily life in smart cities including the smart grid. The proposed botnet detection framework collects network traffic flows and converts the connection records using DL methods on a dataset for detection. The results revealed the DL classification model's outperformed the ML [28]. Schädler et al., (2018) proposed an Agent-based model for simulating Smart Grid innovations by introducing a new market design, market mixes, emerging technological inventions and new regulations to derive indicators for future smart grids. [26]. Acarali et al., (2020) modelled DoS attacks and interoperability in the Smart grid by applying the epidemic principles to explore the dynamics of using susceptible, attack and compromise models on IT and OT systems [27]. Kotenko (2005) explores agent-based modelling and simulation of cyber-warfare between malefactors and security agents on the internet by exploring malefactor ontologies of DDoS attacks [20]. Macal and North (2008) experimented with different toolkits and methods for developing agent-based modelling and simulations [21]. Kotenko et al. (2011) outlined a software framework for agent-based simulation of cooperation defence mechanisms against botnets using an agent-oriented approach at a packet level within a network simulation [12]. Vogt et al. (2007) examined the possibilities of deploying super botnet agents simulating large-scale attacks on networks. The authors explored various botnet vulnerabilities using structured attack algorithms that result in determining the properties of super-botnets in a DDoS environment [13].

Regarding botnet attacks on IoTs, Soltan et al. (2018) explored the impact of large-scale botnets of high wattage on IoT devices and how they disrupt the power grid by using various ML simulation models to demonstrate how manipulation of demand attacks can affect a smart grid operationally [14]. Giachoudis et al. (2019) evaluated a collaborative agent-based detection of DDOS utilizing botnets. The detection method was centred on security on IoT devices and based around the distributed multi-agent system by using an algorithm to simulate and test the proposed agent's architecture on the various IoT devices [15]. Rajab Challo and Kotapalli (2011) proposed a method for detecting and removing botnets using honeypots and P2P botnets by constructing a P2P structured botnet that detects infected honeypots and maligns the network [16]. Sgouras et al. (2017) performed a short-term risk assessment of botnet attacks on advanced metering infrastructure by emulating a DDoS attack in a closed testbed environment using a topology of smart meters that participated in an electricity market. [17]. The proposed method was used to evaluate the impact on such attacks' reliability. Acarali et al. explored the characteristics of smart grid DoS attacks by identifying and analysing sets of specific DoS scenarios that were deployed on smart grid components targeted in the context of the underlying grid infrastructure [18]. Zheng et al. (2022) explored cyberattacks on the smart grid, critical defence approaches and digital twin by integrating intelligence systems, and digital and internet connectivity on CPS to the attack surface [19].

All the existing literature considers ABS, botnet agents and various methods such as NetLogo and CORMAS tools model attacks and are relevant to improving cyber security. However, none of them explored the ABS of botnet amplification attack scenarios using the GAMA tool for

attack modelling to improve smart grid security. Therefore, we use the GAMA tool to simulate smart grid systems to detect botnet interactions. Further, we used the GAMA

III. APPROACH

This section discusses the approach used for the ABS simulation, the attack method and the algorithms for deploying the attacks. We consider how the GAMA tool is used to model the agents for this scenario. The GAMA is a modelling and simulation development environment for building ABM with a spatial focus. The GAMA tool provides an integrated development environment (IDE) and platforms for modelling and simulation that allows developers to switch between building models and simulation visualisations that allow developers to have a deeper impact on the agent habits and processes. [1]. Erdelyi at el. used GAMA to model the transition of mobility towards smart and sustainable cities [18]. The approach implemented in this paper utilizes RStudio software application that provides an IDE and function library for data processing, manipulating, and modelling. We use RStudio to synthesize simulation data and provide objective conclusions on the ABS discussed in this paper.

In our approach agents are designed to emulate the workings of a smart grid with power generation infrastructure. For botnet systems, this helps approximate behaviour for intra-botnet communication.

A. ABS Simulation Control Process using GAMA

Figure 2 discusses the simulation process using the GAMA tool for the implementation. Agents are initialized and deployed on the GAMA tool. We deploy the GAMA tool and the R Analysis Model. In the GAMA simulation model, we specify three parameters referenced in Figure 2.

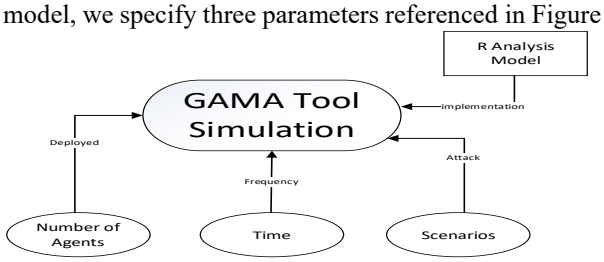

Fig 2. Simulation Control Process

B. Modelling Botnet Attacks Agents on Smart Grid

This section discusses the botnet agents attack modelling on a smart grid environment. A smart grid integrates power generation, transmission and distribution systems using various components in cyber physical, cyber digital and human elements to provide electric power to consumers. The botnet agents include the botmaster agent (BTM) and the bot agents(BTA). Agents that are responsible for creating a virtual EM are the Genco (GenCo), Power Plant (PP), Smart Meter Agent (SMA), Market Operator Agent (M0) and Household Agent.

C. Categories of Botnet Agent Classes

Botnet agent classes can be categorised based on their functionalities in a given scenario. Understanding how botnet agent classes are categorized in terms of how they function can assist in detecting specific threats that they pose in a smart grid environment and could assist in developing a security strategy and control mechanisms to mitigate cyberattacks. IMPLEMENTATION

agent-based simulation tool to model the ABS of botnet volumetric and amplification attack scenarios on smart grid systems.

D. Botnet Agent Volumetric and Amplification Attack

Figure 3 considers how botnet attack agents propagate volumetrically and amplify in the network and affect the entire system. When the simulation setup starts, a simulation scenario is chosen from the array of simulation scenarios. The simulation scenario's first action is to initialize the various probability–related variables. Then the array of scenarios is exhaustively searched in the probability space enumerating all possible combinations. These variables control the occurrence of cyberattacks in the smart grid. Finally, simulation scenarios are executed sequentially. Our simulation ends when all simulation scenarios have been executed. After choosing a scenario, the simulation initializes agents (HA, GenCos, RetailCos, MO, BTM).

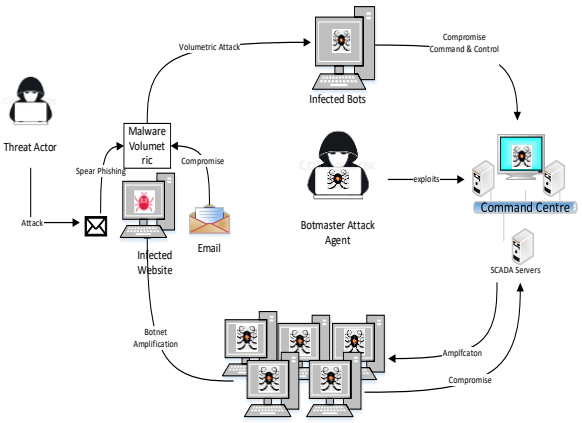

Fig 3. Botnet Agent Volumetric and Amplification Attack

C. Simulation Algorithms

This section discusses the simulation of the algorithms implemented for the models.

E. Algorithm 1: Botnet Command Propagation Algorithm (BCPA)

The BCPA is responsible for sending/requesting commands from the BTM agent to the BTA agent. The algorithm considers how communication occurs in the botnet agent system with a botmaster agent and multiple bot agents. Upon initialization of the simulation experiments, variables are initialized that provide BTM agents with the scope to provide either a pull delivery or a push delivery mechanism to propagate its command to the BTA Agents.

Algorithm 1 PsuedoCode - Botnet Command Algorithm

1: Start,
2: Create a set of bot-master agents from the number in the specified experiment scenario
3: Create bot agents from the specified experiment scenario
4: Specify a probability P1 and P2 from the given distribution from the experiment scenarioo
5: IF P1 returns true , set botnet agents to communicate in a push communication methodology, set P1 == True
6: If P1 == True , set botnet agents to make a request to server, to update current command state
7: Return Pull
8: Else If P2 returns true , set P1 to true and botnets agents will communicate in a pull mechanism, set P2 == True
9: If P2 == True , set botnet agents to overwrite command state with bot master command state, botnet agents make a request to pull commands from bot-master agent

Fig 4. Botnet Command Algorithm Pseudocode

Botnet agents are responsible for maintaining the liveness of their understanding of the botmaster agent in the context of receiving and applying commands. Furthermore, in a smart grid context, this allows for the delivery of cyber-attack algorithms described in Figure 5.

Algorithm 2 Botnet Command Algorithm

global variables
  $Bpull$
  $Bpush$
  Ba
  Bm
  Ss
  Bp
  Exp
end global variables
procedure GAMA EXPERIMENT(BA,Bm,Bp,$ExpS$)
  procedure CHECK$_b$$otmaster_s$$tate$(BA)
Require:

$$Ba! = \emptyset, ExpS! = \emptyset$$

  Initialize Bot-master Agent, (Ba) with random parameters in the search space
  Initialize a population of botnet agents (Bm) with stochastic parameters in the search space
  while Simulation Experiment Termination condition not reached **do**
    for all $i \in (Exp)$ **do**
      if $Bpull$ is selected **then**
        Initiate Pull from Bm , apply check botmaster state
        Check for duplicate messages, discard older messages
        Pull Scenario Variable from Exp
        Confirmation of Pull Send to Bm
      else if $Bpull$ is selected **then**
        Initiate Push from Bm
        Send command updates to Ba
        Update command and metadata

Fig 5. Botnet Command Algorithm Pseudocode

Table 1. Botnet Command Algorithm Pseudocode Descriptive Table

Variable	Description
Bpull	Pull Delivery State
BPush	Push Delivery State
Ba	Set of Botnet Agents
Bm	Set of Botmaster Agents
Ss	Set of parameters for executing scenarios such as FDIA, DDOS
Bp	Boolean State describing whether Bm interacts with Ba by pulling/pushing commands
Exp	Probability Matrix that describes various experiment scenarios

Figure 6 presents the FDIA algorithm that is deployed on the smart grid to penetrate the network. FDIA can be used by the attacker to compromise smart grid measurements within sensors and actuators from the smart meters, by margins that aim to be undectable to bypass the sensor's detection mechanisms. Methodologies in implementing FDIA can stem from a threat actor enumerating database servers, checking and breaking authentication mechanisms through password cracking through a pre-determined seed list, and exploiting misconfigured servers. Once a threat actor gains access to a database server, the opportunities to perform privilege escalation can further exploit misconfigured infrastructure. Furthermore, through insecure and exposed legacy databases, passwords can be enumerated from database servers to provide an attacker access to the user account. That may enable masquerading as legitimate users and maliciously writing/reading faulty data.

Algorithm 3 False Data Injection Attack

global variables
  $rngseed$
  Vpp
  Fpp
  $dmodpp$
  $fdiasm$
  $fdiaed$
  $fdiapp$
  Bm
  Ss ($fdiasm$,$fdiaed$,$fdiapp$)
  $cmdtargets$
  $cmdrepeats$
end global variables
procedure GAMA EXPERIMENT(BA,Bm,Bp,$ExpS$)
  procedure CHECK$_b$$otmaster_s$$tate$(BA)
Require:

$$Bm! = \emptyset, ExpS! = \emptyset$$

  Initialize Bot-master Agent, (Ba) with random parameters in the search space
  Initialize a population of botnet agents (Bm) with stochastic parameters in the search space
  while Simulation Experiment Termination condition not reached **do**
    for all $i \in (Exp)$ **do**
      for all $i \in (Ss)$ **do**
        if $fdiasm$ is selected **then**
          Find all Smart Meter agents
          Enumerate number of targets ($cmdtargets$) and repetition of targets($cmdrepeats$) from commands from Bm
          for $i \leftarrow 1, cmdtargets$ **do**
            Construct a set of targets given by i
            for $i \leftarrow 1, cmdrepeats$ **do**
              Modify energy load per hour via $rngseed$
              if $fdiapp$ is selected **then**
                Find all Power Plant Agents
                Enumerate number of targets ($cmdtargets$) and repetition of targets($cmdrepeats$) from commands from Bm
                for $i \leftarrow 1, cmdtargets$ **do**
                  Construct a set of targets given by i
                  for $i \leftarrow 1, cmdrepeats$ **do**
                    if Agent selected is Vpp **then**
                      Apply dynamic modification energy load procedure
                    else
                      Modify energy load per hour via $rngseed$
                1

Fig 6. FDIA Algorithm Pseudocode

Our implementation works on the premise that a threat actor has already performed reconnaissance and gained access to the network and can perform lateral movement within the smart grid environment similarly.

IV. RESULTS

This section discusses the results of the various botnet agent attack scenarios and their impact on the smart grid. The simulation environment described in section 4 discusses how we run several experiments to understand the effect of amplification on the smart grid operational activities. We propose several scenarios to investigate our research aim and understand how we can investigate the effect of volumetric cyber-attacks in a smart grid environment.

A. Power System Power Plant FDIA Attack

The study observes from Figure 7 depicts a low probability of power plants experiencing an FDIA attack, producing data points, that are clustered close together, and consequently have a low standard deviation. As the response variable variables increase against defined ranges, the dispersion of the predictor variable produces an effect. When an FDIA attack occurs in the power plant system, it distorts real energy demand and supply figures in the experiments, so inducing a smart-grid resource to over-produce or under-produce. Figure 7 has little or no correlation at low intervals with the predictor variable, this makes the case that at low intervals traces of FDIA manipulation can be undetected and remain dormant in a smart grid environment. However, at high values, the impact of FDIA manipulation can be observed. From the results provided, there is a linear correlation between a

power plant's electricity price per hour and the impact of FDIA probability is seen. Even small amounts of amplification produce an effect on the response variable.

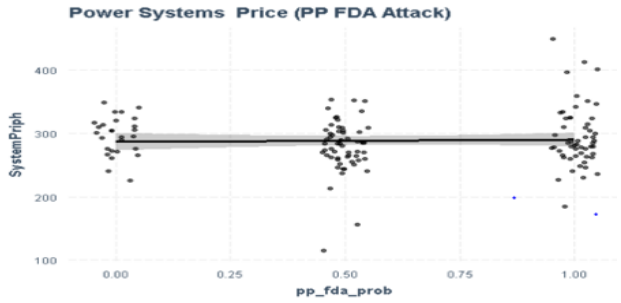

Fig 7: Power System Power Plant FDIA Attack

The experiment referenced in Figure 8 constructs an experimental scenario, in which the rigour of establishing a correlation between a power plant FDIA attack probability and the corresponding effect of electricity traded. It is observed that although a PP FDIA attack aims to manipulate a power plant's electricity loads and has an effect on increasing the standard deviation of the electricity. It's observed that this metric is stable for subsequent iterations of variations of the response variable.

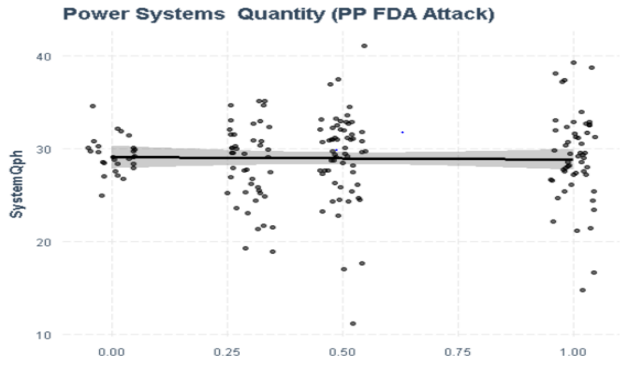

Fig 8: Power System Power Plant FDIA Attack - AEQH

From our simulation-derived regression model, it seems that FDIA attacks centred on smart meters in contrast to power plants have a greater tilt in producing instability in the electricity market. FDIA manipulation within power plants is less significant within our implementation, as power systems (agents for a collection of power plants) try to split the AHEL between all sub-power plants. In comparison to the SM FDIA attack routine, SM agents then submitted to the market operator, two other variables that experience similar effect significant variables that are of interest are market operator FDIA probability and. It is observed when the FDIA probability is increased, a slight increase is observed.

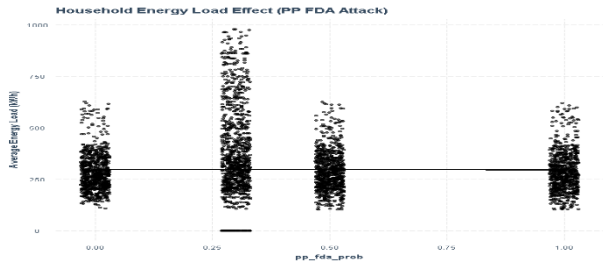

Fig 9: Household - Power Plant FDIA Attack – AEQH

V. EVALUATION

This section considers the evaluation of the simulation model, motivating and the discussion of the behaviour modelling, and the data architecture model. Regarding the evaluation of Behaviour Modelling, the simulation model of the smart grid is inherently limited and will need to be extended in the future. In consideration of the networking layer, our model simplifies the networking layer of the smart grid environment.. Figure 10 depicts the various scenarios that explain each attack graph and its cascading impacts and how the botmaster agents attack other systems that are connected to the network.

1. Botmaster Agent exploits vulnerabilities and could penetrate the network and initiate a malware attack to cause volumetric and amplifications as shown in Figure 5 algorithm to impact the smart grid.
2. FDIA: Cyber Attack Probabilities (Scenario vs change in electricity price per meter to a customer, reading per meter) leading to loss of earnings company.
3. Effect of Demand Response (impact of DoS attacks) during peak times and off-peak times
4. Botnet Agent causes DDoS amplification effect on the smart grid to affect different user outcomes.
5. Botnet Agent FDIA amplification effects on different household agents as discussed in section A in the implementation.
6. Botmaster agent to take command and control of the system to manipulate the system
7. Impact of cyberattacks on the distribution system to cause oscillation attacks and price fluctuations.

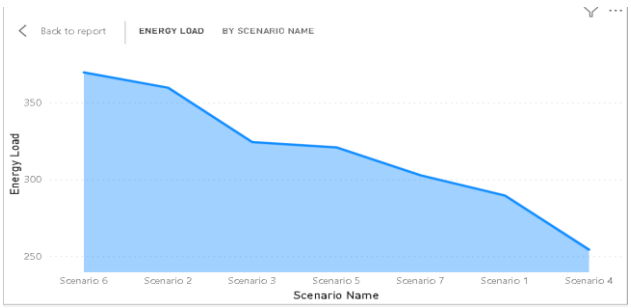

Fig 10: Attack Scenarios

Our simulation model shows how we implemented the amplification of botnet attacks by approximating application layer DDoS attacks. Consequently, defensive/offensive actions taken by attackers or defenders can't be fully simulated in our current approach. Additionally, our model assumes that messaging between agents is unauthenticated, another layer of adding more realistic behaviours to agents would be providing an authentication layer to agents, to understand how amplification and cyber-attack patterns can reveal flaws with authentication protocols with smart grids. Additionally, our simulation model can be further improved by the inclusion of FDIA detection agents. The FDIA detection agents were constructed in the implementation, to detect the effect of its significance instructions of the bots agent due to the degree of damage and its cascading impact on the smart grid. Exploring the effect of FDIA detection agents as a form of security detective controls could be very practical to explore in further detail. Regarding the implementation of the MO agent, it provides the MO agent to alert agents to anomalous behaviour, to perform resubmission of electric orders, and remove from orders that are detected to be anomalous traffic. Finally, our simulation model makes a clear assumption, that an attacker is already inside the network, and possesses a way to compromise the smart grid

system. Botnet agents are designed to exploit software vulnerabilities and unpatched updates. To prevent these exploits, we recommend regular updates to antivirus and anti-malware as malicious botnet agents are difficult to detect. Install anti-spam and anti-phishing detection tools and mechanisms to mitigate the botnets. One of the basic approaches to mitigating malicious bots is training staff and creating awareness of the dangers of accessing spam or phishing emails.

VI. CONCLUSION

Due to industrial dependencies on smart grid systems to enhance economic growth, innovations and sustainable development, the paper has provided botnet attack simulation using ABS for DoS attacks for security improvement using GAMA tool to harness technological advancements toward the 17 UN-defined SDGs specifically required action to take that will affect outcomes on goals 8 and 9 in development and environmental sustainability.

As discussed, ABS modelling describes a set of experiments involving botmaster agents and how it deploys bots in the networks to cause FDIA and DDoS attack modelling and how the other agents react to that and the results of the defence mechanisms. The paper has discussed the state-of-the-art and the related works of ABS and the botnet agent attack surface including the various methods deployed in the simulation of complex adaptive systems that focused on emergence and heterogeneity of the smart grid environment. Further, we have discussed the approach used for the application of agent-based simulation and how the development environment was constructed as well as the GAMA tool and the R script used for the implementation and the regression analysis. Furthermore, we have implemented the ABS simulations for the various models and have considered how attacks a deployed using various algorithms for the classification of the botnet agents and attack modelling designed to explore the FDIA and DDoS attack goals. Finally, we discussed the regression analysis results and recommend a control mechanism to improve smart grid security.

Future work will consider modelling ABS simulations to predict attacks from different oscillation attacks in an extreme power distribution for performance evaluations.

REFERENCES

[1] D. Patrick Taillandier, "Building, composing and experimenting complex spatial models with the GAMA platform," GeoInformatica, 2018.

[2] M. Bae Jang Won, "Combining Microsimulation and Agent-based Model for Micro-level Population Dynamics," Procedia Computer Science, vol. 80, pp. 507-517, 2016.

[3] T. Salamon, (2011) "Design of Agent-Based Models", Lightning, 2011. https://www.walmart.com/ip/Design-of-Agent-Based-Models-9788090466111/53665715

[4] G. Tina Balke, "How Do Agents Make Decisions? A Survey," Journal of Artificial Societies and Social Simulation, vol. 17, no. 4, p. 13, 2014.

[5] E. Manfred Pochacker, Simulating the Smart Grid, Arvix, 2013.

[6] F. Philipp Ringler, "Agent-based modelling and simulation of smart electricity grids and markets – A literature review," ELSEVIER, pp. 205-215, 2016.

[7] N. C. Wadhawan Yatin, "A Comprehensive Analysis of Smart Grid Systems against Cyber-Physical Attacks," Electronics, vol. 7, no. 10, p. 249, 2018.

[8] F. Aloul, "Smart Grid Security: Threats, Vulnerabilities and Solutions," SGCE, 2012.

[9] K. Ahmed, "False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure," Complex Adaptive Systems Modeling, vol. 8, no. 1, p. 4, 12/2020.

[10] H. Ramzy Shaaban, "TCP and HTTP Flood DDOS Attack Analysis and Detection for space ground Network," in 2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Cairo, Egypt, 2019.

[11] G. Foreman James Christopher, "Cyber Attack Surface Analysis of Advanced Metering Infrastructure," p. 9.

[12] I. Kotenko, "Agent-based simulation of cooperative defence against botnets," Concurrency and computation, 2011.

[13] J. J. Ryan Vogt, "Army of Botnets," in Proceedings of the Network and Distributed System Security Symposium, San, 2007.

[14] W. L. Guofei Gu, "BotSniffer: Detecting Botnet Command and Control Channels," Atlanta.

[15] R. E. Jean-Paul Zimmermann, "Household Electricity Survey: A Study of domestic electrical product usage," Intertek Testing & Certification Ltd, London, 2012.

[16] M. z. Gunduz, and P Das (2020). "Cyber-security on smart grid: Threats and potential solutions". Computer Networks. 169, 107094. https://doi.org/10.1016/j.comnet.2019.107094

[17] M. Toshpulatov and N. Zincir-Heywood, "Anomaly Detection on Smart Meters Using Hierarchical Self Organizing Maps," 2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), ON, Canada, 2021, pp. 1-6, doi: 10.1109/CCECE53047.2021.9569097.

[18] M. Dharmesh Faquir, "Cybersecurity in smart grids, challenges and solutions," AIMS Electronics and Electrical Engineering, vol. 5, no. 1, pp. 21-37, 2021.

[19] F. Lopes, Electricity Markets with Increasing Levels of Renewable Generation: Structure, Operation, Agent-based Simulation, and Emerging Designs, Springer, 2018.

[20] I. Kotenko "Agent-Based Modeling And Simulation Of Cyber-Warfarbetween Malefactors And Security Agents In Internet" 2005. Proceedings 19th European Conference on Modelling and Simulation.

[21] C. M. Macal and M. J. North (2008). "Agent-Based Modeling And Simulation: ABMS Examples" IEEE. Proceedings of the 2008 Winter Simulation Conference.

[22] A. Yeboah-Ofori, J., Abdulai, and F., Katsriku (2019) "Cybercrime and Risks for Cyber Physical Systems. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2019. 8(1), 43-57. pp43-57. https://doi.org/10.17781/P002556

[23] J. Erdelyi, "Simulating the transition of mobility toward smart and sustainable cities," HAL open science, pp. 1-5, 2021.

[24] A. Yeboah-Ofori and S. Isam 2019. Cyber Security Threat Modelling for Supply Chain Organizational Environments. MDPI Future Internet 2019, 11(3), 63; https://doi.org/10.3390/fi11030063

[25] Akhatova, L, Kranzl, F. Schipfer, C.B. Heendeniya, (2022) "Agent-Based Modelling of Urban District Energy System Decarbonisation—A Systematic Literature Review". *Energies* 2022, *15*, 554. https://doi.org/10.3390/en15020554

[26] P. Schädler, H. Wache and E. Merelli, (2018) An Agent-Based Model for Simulating Smart Grid Innovations, *2018 15th International Conference on the European Energy Market (EEM)*, Lodz, Poland, 2018, pp. 1-5, doi: 10.1109/EEM.2018.8469939.

[27] D. Acarali, M Rajarajan, D. Chema, and M. Ginzburg, (2020). "Modelling DoS Attacks & Interoperability in the Smart Grid". 2020 29th International Conference on Computer Communications and Networks (ICCCN), doi: 10.1109/icccn49398.2020.9209671

[28] S. Sriram, R. Vinayakumar, M. Alazab and S. KP, "Network Flow based IoT Botnet Attack Detection using Deep Learning," *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Toronto, ON, Canada, 2020, pp. 189-194, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162668.