MANCHESTER
1824

The University of Manchester

Security of Substation Information in Energy Networks Using the Markov Decision Process

A thesis submitted to The University of Manchester for the degree of

Master of Philosophy

in the Faculty of Science and Engineering

2022/2023

Jiangxin Lyu

10913447

Supervised by:

Prof Zhirun Hu

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING

CONTENTS

Word count: 12298

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACK	Acknowledgement (data networks)
ACSI	Abstract Communication Service Interface
ARP	Address Resolution Protocol
CB6	Carbon Budget 6
CCC	The Climate Change Committee
CPS	Cyber-Physical System
DDoS	Distributed Denial of Service
DNS	Domain Name System
EEI	The Edison Electric Institute
FDIA	False Data Injection Attack
FIN	End Flag
GOOSE	Generic Object-Oriented Substation Event
HMI	Human-Machine Interface
HTTP	The Hypertext Transfer Protocol
ICMP	The Internet Control Message Protocol
ICT	Information and Communication Technology
IED	Intelligent Electronic Devices
IGMP	The Internet Group Management Protocol
IOS	IPhone OS
IoT	Internet of Things

IP	Internet Protocol
MAC	Message Authentication Code
MC	Markov Chain
MDP	Markov Decision Process
MITM	Man-In-The-Middle
MMS	Manufacturing Message Specification
MRP	Markov Reward Process
MU	Measurement Unit
LAN	The Local Area Network
LAND	The Local Area Network Denial
LN	Logical Nodes
OSI	The Open Systems Interconnection model
PSH	Push Flag
RST	Reset Flag
TCP	The Transmission Control Protocol
SAS	Substation Automation System
SCADA	Supervisory Control And Data Acquisition
SSL	Secure Sockets Layer
SV	Sampled Value
SYN	Synchronization Flag
URG	Emergency Sign

Abstract

In recent years, as the amount of new energy production has steadily increased and new technologies have developed rapidly, energy networks have increasingly become more diverse and intricate. Being a vital social infrastructure, the smart grid will confront a growing number of network security risks as a result of the complicated network security environment and competing interests. Taking into account the significance of information security in the energy network and the need for its safe and stable operation, this research employs modelling and simulation to examine the security risk of smart substations when the network is under cyber-attacks.

On the basis of the preceding background, this report first enumerates and analyses prevalent network attack methods and risk assessment methodologies in energy networks, and then determines the necessary components based on the features of smart substations. Second, this study analyses the probabilities of state transitions under various assault pathways. Lastly, a network assault model of smart substation based on the Markov Decision Process is developed from the standpoint of the attacker, and the solution analysis for network security risk assessment is conducted.

Key words: Markov decision process, cyber security, digital substation, energy network

Declaration

I hereby declare that the work contained in this dissertation, has not been submitted for any other award and that it is all my own work. I also confirm that this work uses ideas and opinions from written papers and articles from the work of others.

Name: Jiangxin LYU

Signature: Jiangxin Lyu

Date: 2023/10/21

Copyright Statement

The author of this thesis (including any appendices and/or schedules to this thesis) owns certain copyright or related rights in it (the “Copyright”) and they have given the University of Manchester certain rights to use such Copyright, including for administrative purposes.

Copies of this thesis, either in full or in extracts and whether in hard or electronic copy, may be made only in accordance with the Copyright, Designs and Patents Act 1988 (as amended) and regulations issued under it or, where appropriate, in accordance with licensing agreements which the University has from time to time. This page must form part of any such copies made.

The ownership of certain Copyright, patents, designs, trademarks and other intellectual property (the “Intellectual Property”) and any reproductions of copyright works in the thesis, for example graphs and tables (“Reproductions”), which may be described in this thesis, may not be owned by the author and may be owned by third parties. Such Intellectual Property and Reproductions cannot and must not be made available for use without the prior written permission of the owner(s) of the relevant Intellectual Property and/or Reproductions.

Further information on the conditions under which disclosure, publication and commercialisation of this thesis, the Copyright and any Intellectual Property and/or

Reproductions described in it may take place is available in the University IP Policy, in any relevant Thesis restriction declarations deposited in the University Library, the University Library’s regulations and in the University’s policy on the Presentation of Theses.

Acknowledgements

First of all, I would like to convey my gratitude to my supervisor, Professor Zhirun Hu. During my MPhil studies, Prof. Hu offered me invaluable assistance and counsel. He is both academically and humanly admirable in my eyes. His kindness and patience like a spring breeze cares my heart throughout all times.

Secondly, I would also like to convey my thanks to my co-supervisor, Dr Haiyu Li, for his kind assistance and academic mentoring. In addition, I would like to thank Zhihao Wu for his meticulous help.

Lastly, I want to express my appreciation to my parents for their constant support and encouragement.

1. Introduction

1.1 Background

Since the 21st century, with the rapid development of industrialisation, electricity demand has grown enormously. With the continuing energy crisis caused by the depletion of fossil resources and the rising demand for energy on a global scale, the production of electricity on a global scale is currently encountering considerable challenges. The expansion of the economy leads to a rise in the amount of energy utilization and environmental deterioration. Consequently, decarbonisation of the energy network is becoming critical as climate and environmental threats become more serious. The Climate Change Committee (CCC) has issued recommendations for setting carbon budget 6 (CB6) levels, covering 2033 - 2037. The CCC recommends setting CB6 at 965 MtCO2e to reduce emissions by 78% between 1990 and 2035 [1]. It is a common knowledge by now that excessive use of non-renewable resources can lead to significant environmental hazards such as the greenhouse effect. Given the context mentioned earlier and the twin driving force of the energy crisis, it is unavoidable that the future energy structure will shift to new energy. Furthermore, the growth of the energy network in the direction of informatisation, intelligence, and sustainable development is more in keeping with the times than in the pursuit of high efficiency and high stability [2].

Power facilities are regarded as one of the most significant social infrastructures, and the steady functioning of the power system in the energy network is crucial to the orderly growth of the national economy and social peace. Consequently, information security is essential for the safe and stable operation of energy network systems. Providing optimal energy demand management with intelligent grids is a superior solution to the challenges caused by conventional grids. A smart grid can supply consumers with reliable and environmentally friendly electricity, but it also increases power system operations’ reliance on network infrastructure for control and monitoring [3].

In recent years, however, with the continuous increase in the proportion of new energy production and the rapid development of new technologies, the energy network has become progressively more diverse and complex, posing significant challenges to the safe and stable operation. In a complicated network security environment, the energy system's network infrastructure poses a certain level of security risk. The network risks encountered by the electrical system are getting increasingly severe, and the network security concerns it faces have also attracted widespread attention and discussion.

Malicious attacks on energy networks are happening and often cause huge losses. For example, a third party illegally hacked into the computers and SCADA systems of three electricity distribution companies in Ukraine in December 2015, resulting in multiple power outages and approximately 225,000 customers without electricity [4]. A severe safety incident occurred in July 2019 at a nuclear power plant near the city of Yuzhno-Ukraine in southern Ukraine. Several employees connected the nuclear power plant's internal network to the public network in order to mine cryptocurrencies. In Johannesburg, South Africa, a ransomware attack on City Power in July 2019 caused power outages in multiple residential areas. The virus encrypts and wreaks havoc on all databases, applications, web applications, and official websites. Ragnar Locker ransomware infected the Portuguese multinational energy company EDP (Energias de Portugal) in April 2020, and the ransom demanded was as high as USD 10.9 million. The attackers claim that if EDP does not pay the ransom, they will release the confidential information they have obtained to the public [5]. The energy network is integral to modern society's production and way of life, and the losses caused by these malicious attacks are incalculable.

The smart grid is rapidly becoming one of the largest cyber-physical systems (CPS), which integrates the power network and information network, and employs massive sensors, advanced metering equipment, and information communication networks to enable remote access to information and remote control of equipment [6]. A smart grid is a modern electrical or digital information and communication technology, and substation automation of the power distribution system is a crucial component of smart grid technology implementation [7]. Consequently, preventing substation network attacks, effectively assessing network security risks, and mitigating the impact of network propagation risks on intelligent substations are crucial.

This thesis focuses on the analysis and assessment methods of network security risks of intelligent energy networks under data attack scenarios based on pertinent theories. An essential component of the intelligent energy network, the substation automation system (SAS), is modelled using Markov Decision Process theory. On the basis of this model, a network security evaluation framework system is developed to address research gaps and give theoretical support for developing energy network cyber security defensive systems.

1.2 Aims and Objectives

Overall project goal:

The overall goal of this project is to study and build a MDP - based energy network information security model, taking into account the characteristics of substations and smart grids. By solving the MDP model, the optimal action strategy could be obtained to achieve the purpose of network security defence.

Overall objectives:

(1) Study and analyse common network attack methods in energy networks.

(2) Study and analyse the structure of the smart substation.

(3) Theoretical study and model development based on the Markov Decision Process (MDP).

(4) Optimization of action strategies by optimizing the model to ensure the information security of the energy network.

2. Literature Review

With the continuous improvement of digitalisation and informatisation, the energy and information networks have been integrated into a complex network. The energy network composed of information Internet technology and renewable energy is diverse and interactive, and it is a new energy system structure that conforms to the development trend [8].

A smart grid is a completely organic system covering various voltage levels and processes such as power generation, transmission, transformation, distribution, consumption, and dispatching. Energy networks have complex relationships with various aspects of the economy and society [9]. At the same time, there are many emerging hotspots in this field, such as renewable energy in energy networks, distribution management systems, demand side management and energy trading in the electricity market [10-12]. For example, in 2005, an Italian company installed and completed the telegestore project, the earliest and largest smart grid system. The program has been recognized as the first implementation of intelligent grid technologies on a commercial scale domestically, bringing considerable profits [13]. Energy market is gigantic. In 2025 alone, China's electric power system market is projected to reach $112.5 billion [14]. It can be seen that the development of smart grid has been highly valued all over the world. In addition to protecting the environment and bringing convenience to people's lives, this growing field is also full of opportunities.

2.1 Common Security Risks in Today's Internet

The smart grid, a system that combines the information side and the physical side, brings not only new opportunities but also new challenges. Since the concept of the smart grid was put forward, its security issues have been widely discussed. For example, in 2010, the Edison Electric Institute published "Principles for Cyber Security and Critical Infrastructure Protection" to propose the creation of a structure for addressing cybersecurity threats [15]. In 2011, the Cybersecurity and Internet Freedom Act was passed by Lieberman [15] and co-sponsors to improve the "security and resilience of the network and communications infrastructure" in America. In addition, there are several collaborations among academic institutions, national research facilities, consumer organizations, and many more concerned with Cybersecurity and the intelligent grid challenges to promote collaboration and exchange of resources on those problems and to assist in funding industry cybersecurity initiatives. Tim [16] specifically focused on the coming security challenges, especially at the power transmission and distribution level, wrote a white paper. Combining perspectives from cybersecurity and communications, they provided a unique perspective on grid cybersecurity challenges and opportunities. Cyber-related attacks have raised questions about security breaches and their massive impact on critical power system infrastructure. Based on this, it is inevitable to ensure the safe and regular operation of the smart grid.

The following security risks may pose a significant threat to personal privacy and may also cause major social losses [17-23].

- DDoS (Distributed Denial of Service): DDoS refers to hostile behaviours that overwhelm a target server or its infrastructure that surrounds it with massive amounts of Internet traffic in order to disrupt the regular operation of the targeted [17]. This attack is the most common and continues increasing in intensity, damage and volume. Various compromised IT infrastructures are used as sources of attack traffic in a DDoS attack. Exploited machines may include both computers and other connected resources, such as Internet of Things devices [19]. The DDoS assault might be compared to a highway traffic jam preventing regular vehicles from reaching their final location.

Denial of service attacks mainly occurs at the application layer of the Open Systems Interconnection (OSI) model because the application layer can send and receive data [19]. In addition, the OSI model has some security protocols in the network layer and transport layer, such as TCP, SSL, IPv6, etc., which are also vulnerable to attacks [18][19]. Figure 1 below is the model of the OSI.

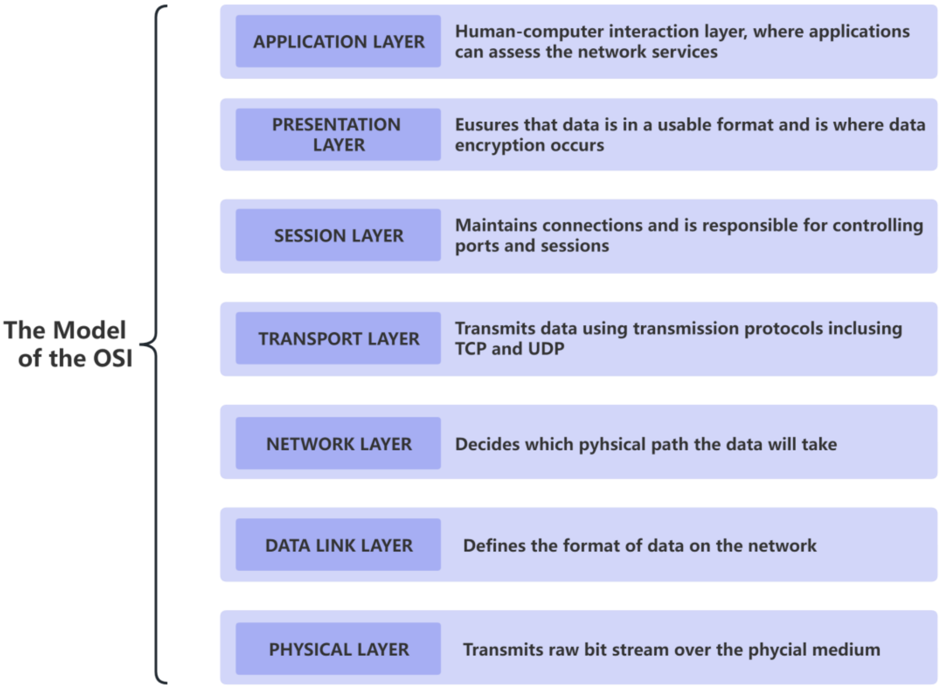

The Model of the OSI
APPLICATION LAYER
Human-computer interaction layer, where applications can assess the network services
PRESENTATION LAYER
Eusures that data is in a usable format and is where data encryption occurs
SESSION LAYER
Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER
Transmits data using transmission protocols inclusing TCP and UDP
NETWORK LAYER
Decides which pyhsical path the data will take
DATA LINK LAYER
Defines the format of data on the network
PHYSICAL LAYER
Transmits raw bit stream over the phycial medium

Figure 1. Model of the OSI [22]

Typical DDoS assaults can be classified into the following categories:

(i) Application layer attacks. The goal of these attacks is to deplete the target's resources in order to cause a denial of service [18]. Figure 2 is an illustration of an application layer assault.

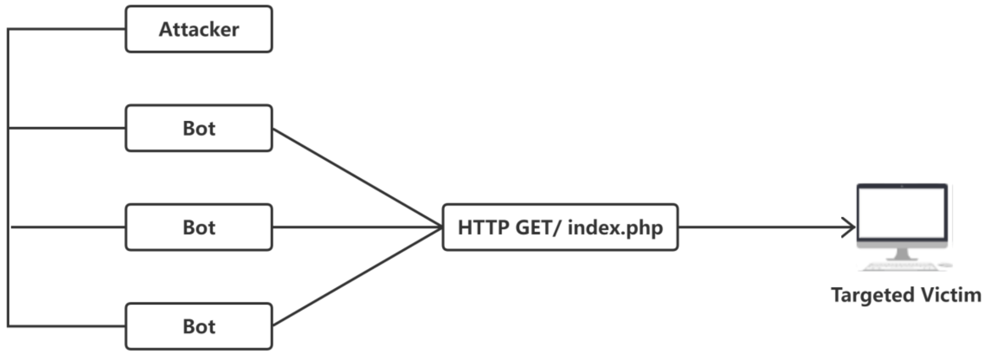


Figure 2. An example of application layer attacks [20]

HTTP flood - This attack is comparable to repeatedly refreshing a web browser on several computers - flooding the server with HTTP requests, and causing a denial of service. Attacks of this type range from simple to complex. A more straightforward implementation might visit a URL with a similarly broad range of attacker internet protocol addresses, referrers, and user agents. Advanced variants may employ a vast number of attacking IP addresses, in addition to unpredictable referrers and user agents, to target random URLs [17-19].

(ii) Protocol attacks. This kind of assault mainly causes service interruption by excessive consumption of server facilities or network device resources. Protocol assaults exploit vulnerabilities in protocol stack layers 3 and 4 to render targets unreachable. Figure 3 below is an example of a protocol attack.

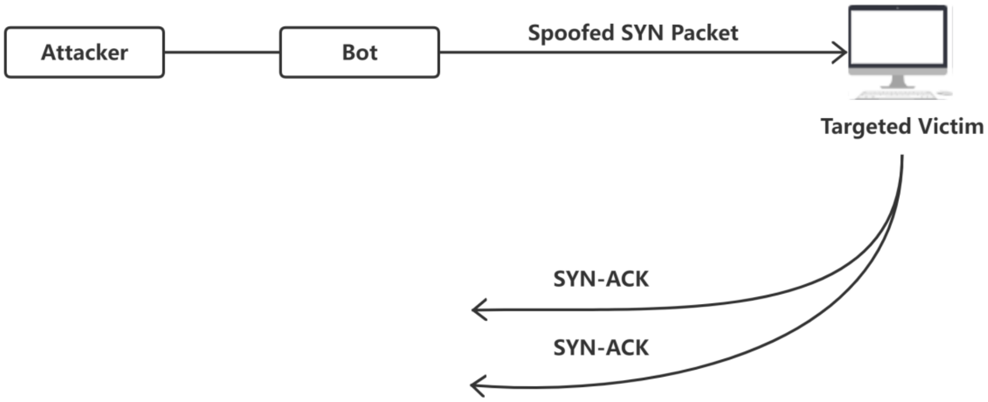


Figure 3. An example of protocol attacks [20]

SYN flood - The assault leverages the TCP handshake — the chain of interactions by which two devices establish an internet connection — by sending a large number of fake TCP "Initial Connection Request" SYN packets to the target [17-19].

The target computer exhausts its resources by responding to every connection request and then waiting for the last phase of the handshake, which never occurs.

(iii) Volumetric attacks. Such attacks aim to induce congestion by utilising all available bandwidth between the victim and the superior Internet. Sending enormous amounts of information to a destination by the use of amplified forms or alternative methods of generating high volumes of traffic. Figure 4 below is an example of volumetric attacks.

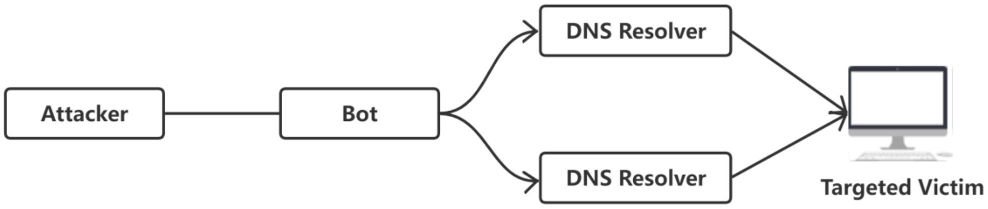


Figure 4. An example of volumetric attacks [20]

DNS Amplification - target IP address then obtains a reply from the open DNS server by submitting a request with a spoofed IP address of the victim.

The most noticeable sign of a DDoS assault is the unexpected sluggishness or inaccessibility of a website or service. Nevertheless, comparable performance issues can have various causes, thus further analysis is typically required. Traffic analysis tools can assist individuals in identifying specific indicators of a DDoS assault [17-19]:

(i) Suspicious traffic emanating from a single IP address or IP range

(ii) High levels of traffic from customers who share a specific behavioral characteristic, like the device type, geographic spot, or internet browser version

(iii) Unexpected surges in the amount of requests to one page or version of an endpoint

(iv) Odd traffic patterns, like spikes or seemingly unnatural patterns at unconventional times of the day.

Since the intelligent grid adopts a distributed architecture system and distributes connections to countless devices, it will suffer huge losses if a DDoS attack is carried out on the grid.

- Phishing Attack: Phishing is a typical technique for social engineering used to steal sensitive user information, like login credentials and payment card information. It occurs when an attacker appears as a reputable entity and persuades a victim to click on an email, instant message, or text message [20]. Subsequently, the user is tricked into clicking a dangerous link, which may end in the installation of malware, the freezing of the computer in a ransomware attack, or the revealing of sensitive information [18][20].

The following is the flow of one of the most common phishing attacks:

(i) A spoofed email ostensibly from within the business is distributed to as many company employees as possible.

(ii) The email states that employees need to update their personal information within three days and attaches a deceptive link.

(iii) Clicking on this link could lead to the attacker monitoring the page and hijacking the employee's password to gain access to the corporate internal network.

- FDIA (False Data Injection Attack): FDIA is a well-planned form of data attack in which an adversary can affect the computing power of the control centre by modifying the raw measurements provided by these sensors. The ubiquity of modern power systems has made IoT sensors one of the critical attack vectors for FDIA attacks [17]. There are two main types of FDIA attacks [20][21]: (i) Insider attacks. An attacker can acquire precise information about the target system's network structure, capacity, costing function, and standard measurements. (ii) External Attacks. Attackers use incomplete power network information to carry out false data injection attacks. As a result, attackers exploit vulnerabilities in the physical network's safety model in order to eavesdrop, replay, and insert false data into the intelligent grid. Targeting holes in input validation and transport layer safety by sending fake data using techniques like code injection and cross-site request forgery is a frequent method for executing such attacks.

An FDIA attack on a power system running on a smart grid can lead to loss of management of control equipment, resulting in huge losses. A German power, chemical, and industrial control facility identified the Stuxnet malware in 2010. The virus aimed at PCS 7 and Simatic WinCC software, and it was identified and fixed before the Trojan could cause significant damage to any financial or real-time data aggregation operations [21]. Nevertheless, there are also many successful cases. For example, an employee of a company that installs radio-controlled sewage plants provided fraudulent data to the sewage plant via radio commands simply because of a negative relationship with the company. This action caused the release of eight million litres of raw sewage into neighbouring parks, rivers, and residential regions, severely impacting the environment and the daily lives of people [20][21]. In addition, in 2015, Ukraine’s electronic power grid system was hacked and installed malware using spear phishing technology, causing 30 substations to lose connection for more than 3 hours, causing incalculable losses.

- MITM (Man-In-The-Middle): This is a kind of eavesdropping attack. An attacker intercepts and distributes messages among two parties who consider they are conversing directly [20]. Among them, the attacker intercepts and then controls the entire conversation in the middle. The attacks seriously threaten online security by allowing attackers to obtain and manipulate private data instantaneously, like login credentials, account information, and payment card numbers. Information obtained during an assault could be used for a variety of malicious objectives, such as identity theft, unauthorised movement of funds, and unauthorised password changes. Figure 5 below is a schematic diagram of the process of a man-in-the-middle attack.

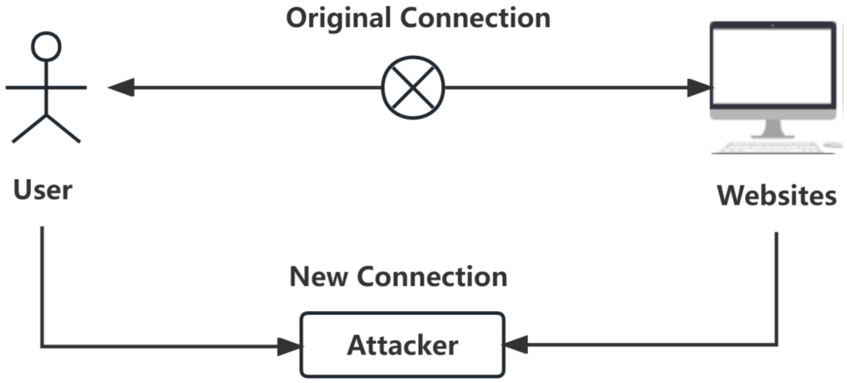


Figure 5. An example of man-in-the-middle attacks [20]

In recent years, there have been quite a few MITM attacks. For example, in 2011, the Dutch registrar website DigiNotar was compromised, which allowed threat actors to access 500 certificates from Google, Skype, and others. Access to these credentials allows attackers to masquerade as legitimate websites in MITM attacks, stealing user data after tricking users into entering their passwords on malicious mirror sites. DigiNotar eventually filed for bankruptcy due to violations. In 2015, it was discovered that the preloaded adware programme Superfish on Lenovo computers scanned SSL traffic and inserted phoney certificates, permitting third-party eavesdroppers to monitor and divert encrypted inbound traffic. On encrypted pages, fake certificates may additionally include ads. In 2017, significant vulnerabilities were identified in the mobile banking applications of numerous well-known banks, leaving IOS and Android users vulnerable to man-in-the-middle attacks. The vulnerability is connected to the certificate pinning strategy used to prevent the use of fake certificates, where security testing is unable to recognize hackers because certificate pinning conceals a lack of effective hostname verification. This finally makes the MITM attack possible.

Generally, (i) data interception and (ii) decryption comprise the two-step technique utilised in these attacks. During data interception, a hacker intercepts a data transmission between the user and a server. While the client and server think they are exchanging information, the attacker intercepts the data, connects to the actual website, and acts as a proxy to read and insert erroneous data into the dialogue [20].

To get access to machines and sensitive data, common MITM attack methods include the following eight techniques:

(i) IP spoofing. Attackers masquerade themselves as applications by changing packet headers in IP addresses. Therefore, users are duped into transferring sensitive information they share during transactions to cyber criminals.

(ii) Domain Name System spoofing. A hacker who invades a DNS server and modifies the address records of a website causes users attempting to visit the site to have the changed DNS records sent to the attacker's site. The primary purpose of DNS spoofing is to redirect traffic to bogus websites or steal user credentials.

(iii) HTTPs spoofing. HTTPs signify a secure and trusted website. Upon the initial connection request to a protected website, HTTPs spoofing sends a false certificate to the user's browser. Attackers can then use this to monitor user interactions and steal shared personal information.

(iv) SSL hijacking. SSL is a technology used to establish a secure connection between the internet browser and an internet server. SSL hijacking happens when a hacker passes fake authentication keys to people and apps during the TCP handshake.

(v) Email hijacking. Cybercriminals can monitor transactions made by users by taking control of email accounts of relevant organizations.

(vi) Wi-Fi eavesdropping. This sort of assault is one of the risks offered by public Wi-Fi networks. Attackers deceive public Wi-Fi users into linking to hostile Wi-Fi networks by establishing Wi-Fi connections with names similar to those of nearby businesses.

(vii) Session hijacking. Attackers profit by stealing personal data and passwords stored in a user's browsing session cookie.

(viii) Address Resolution Protocol (ARP) poisoning. This attack is also called Cache poisoning.

The attacker uses forged ARP messages to connect the hacker's MAC address with the IP of a legitimate user on the LAN to eavesdrop on all traffic routed between them.

- Modification Attacks: Modification Assaults include the manipulation of our assets. Such assaults might be regarded mainly as integrity attacks, but they could also be availability attacks. If attackers get illegal access to a file and modify the information it contains, they have compromised the file's data integrity.

- Malformed Packet Attacks: A malformed packet attack happens when erroneous IP packets are sent to a targeted system, leading the system to malfunction or crash. The equipment with the capability to combat such attacks can recognise and reject erroneous packets in real time.

The following categories malformed packet assaults:

(i) IP Null Payload Packets

A null payload IP packet has one IP header and no data field. When such an IP packet is processed by a target system, the system may malfunction or crash. When enabling protection against malformed packet assaults, a gadget quickly removes such packets.

(ii) IGMP Null Payload Packets

An empty IGMP payload packet has fewer than 28 bytes, which includes a 20-byte IP header plus an 8-byte IGMP payload. When an internet device analyses IGMP packets with a null payload, the device could encounter problems or crash. After enabling protection against malformed packet assaults, the device immediately discards incoming IGMP null payload packets.

(iii) LAND Attacks

The attacker transmits a SYN packet by using the weakness in the TCP three-way handshake procedure. These packets have the same source and destination as the host to which they are addressed. After receiving a significant number of these packets, the target host will establish a large number of empty TCP connections, causing a waste of network resources and possible system failure. After enabling protection against malformed packet assaults, the system verifies the source and destination addresses of SYN packets. The device will remove these packets as they are flawed.

(v) Smurf Attack

An attacker transmits an ICMP Request packet with the target host's source address and the target network's broadcast address as the destination. After receiving the ICMP Request packet, all hosts on the target network transmit the target host ICMP response packets [17-23]. The target host receives a large number of packets, depleting numerous system or network resources and causing failure. When enabling protection against malformed packet assaults, the device verifies if ICMP Request packets contain broadcast or subnet broadcast destination addresses. When a device detects that ICMP Request packets' destination addresses are broadcast or subnet broadcast addresses, it eliminates the packets.

(vi) Attacks from Packets with Invalid TCP Flag Bits

Six flag bits make up a TCP packet: URG, ACK, PSH, RST, SYN, and FIN. Various systems react differentially to this flag bit combined.

a) The assault is a Christmas tree attack if the six flag bits are set as 1. Devices vulnerable to the Christmas tree assault may malfunction.

b) A hacker transmits one TCP packet with SYN and FIN values of 1 to a target host. In response to a deactivated receiving port, the receiving device sends an RST | ACK signal. The receiver will react with SYN | ACK if the receiving interface is enabled. This method is utilized to determine if the host is online and whether an interface is allowed.

c) A hacker transmits one TCP packet with all flag bits are set to 0. If the receiving interface fails to operate, the receiver will respond with one RST | ACK message to figure out if the host is online. If the receiving interface is activated, Linux and UNIX operating systems do not reply, while Windows operating systems answer with one RST | ACK message. The approach is utilized to determine the computer system of the target host.

After enabling protection against malformed packet attacks, the equipment verifies every single flag bit in TCP packets to prevent cyberattacks with packets containing incorrect TCP flag bits. When one or more of these circumstances are satisfied, TCP packets are discarded:

a) Each of the six flag bits is a 1.

b) Both the SYN and FIN bits are ones.

c) Each of the six flag bits is a 0.

- Relay Attack: This kind of cyberattacks is resembled by MITM attacks. In contrast to MITM assaults, in a traditional relay attack, the hacker initiates contact with both parties and passes messages between them without altering or viewing them. Typically, Attackers could get the degree that the signal is boosted. Intruders steal the contents of communication (such as an authentication message) and transmit it to its intended recipient. For instance, a criminal may collect the signal from a user's remote control for a keyless front door, store it, and use it when the person is absent. Another instance is when an attacker intercepts credentials transmitted from a network user to a host and re-uses them to obtain access to the server, thus confounding the host and establishing a new session for the attacker.

2.2 Cybersecurity Risk Assessment Methods

The core focus of this report is to investigate the information security for the active and flexible energy network. This section will discuss, compare and learn from the commonly used cybersecurity risk assessment methods.

Karimipour [24] proposed a robust state estimation algorithm against FDIA in 2017. It reviews research demonstrating cybersecurity risks and builds solutions to enhance grid security. A robust predictive control algorithm is suitable for inaccurate models and can effectively suppress disturbances. However, the intense conservatism of this algorithm is its main drawback. Vernotte [25] conducted a cybersecurity assessment of the ICT component of the smart grid. This study is based on the intelligent grid standard structure model centred on load balancing that was designed as a component of the assessment with the assistance of SCADA systems and intelligent grid experts. Nevertheless, this article is primarily concerned with the load balancing of green energy sources. It is to ensure the stability of the grid by balancing the production and consumption of renewable energy and avoiding regional congestion. There are many other functions in the domain of information security for intelligent grids that need to be analysed and possibly compared with each other. Kimani [26] explores the main obstacles and security concerns hindering the development of intelligent energy networks via the IoT. It is suggested to use the quickest method for detecting intrusions to detect fake data injection incidents in smart electricity systems featuring time-varying dynamic models. Ferrag [27] conducted an exhaustive review of existing cybersecurity approaches for electrical grid SCADA systems on the basis of fog. Kuljeet, Georges, and Sherali [28] chose blockchain-based technology to secure energy network information. Blockchain technology has the characteristics of decentralization and data stabilisation, so the recorded information depends on its authenticity and reliability. The smart grid network security defence system designed based on this technology can effectively guarantee the confidentiality and integrity of user data. Yet, the technology is still in its infancy in laboratory development and faces obstacles in its application.

These articles utilise a variety of theories and methodologies. Using a variety of techniques and theories to protect energy networks serves a similar aim. Markov decision process (MDP) as one discrete-time stochastic control process. It offers an algebraic structure for describing selections whose outcomes are partially unpredictable and partially under the decision-control. In addition, MDPs are valuable for analysing optimization difficulties addressed by dynamic programming, in which costs are minimised or, equivalently, rewards are maximised when applied correctly. Thus, the author of this thesis selected the more mature and dependable Markov decision process (MDP) theory, which is more commonly applied in real-world situations.

3. Preliminaries

3.1 Smart grid

With the increase in the public's consciousness of protection on environmental-friendly energy, today's power system must not only deal with uncertain energy demand from consumers but also deal with a complicated and variable energy supply. Traditional power systems rely mostly on thermal power and hydropower, and their power generation is very straightforward to regulate. However, traditional thermal power plants that utilise nonrenewable energy cannot meet the demands of modern society for sustainable energy development and environmental protection [29]. From the standpoint of energy structure, the direction of future development is new energy and the comprehensive usage of new energy; thus, the outcome may alter the organisational structure of the power grid or entirely subvert the present network structure. If viewed from the perspective of development, it will undoubtedly progress towards digitalisation and intelligence. Thus, the incorporation of renewable energy technologies into the grid is imminent and essential. The emergence and ongoing development of different new energy sources, including wind turbines and photovoltaic power stations, have presented new opportunities and difficulties for the development of power systems [11][30].

Based on such circumstances, the concept of intelligent grid has been developed.

3.1.1 Definition and Structure of the Smart Grid

Smart grids enhance the capabilities of conventional grids to supply users with electricity that is dependable, environmentally friendly, and cost-effective. In addition, it increases the power system's dependence on network infrastructure for control and monitoring [3][12]. The smart grid encompasses the increasingly conventional sectors of bulk generation, transmission, distribution, consumers, markets, and power electronics, as well as relatively new areas such as new energy and electric vehicles. In a suitable amount of time and space, smart grid control facilitates interconnection and interaction across these existing and emergent areas.

Essentially, the smart grid is the next-generation energy network that enables distributed generation, distributed storage, and applications for managing demand-side loads, and is economical and sustainable. Features of the smart grid are [12] [31]:

(i) Data flow and information management as the core

(ii) Environmental effect reduced

(iii) Customer engagement and interaction enhanced

(iv) Higher supply security, quality, and reliability

The framework diagram of the smart grid is shown in Figure 6. The smart grid's conceptual model outlines the system's general composition and applications. It presents a high-level perspective of the system that may be comprehended by several stakeholders. The design lays the way for the advancement of intelligent grid technologies of the future generation that use contemporary computing systems such as the Internet, edge computing, and cloud computing.

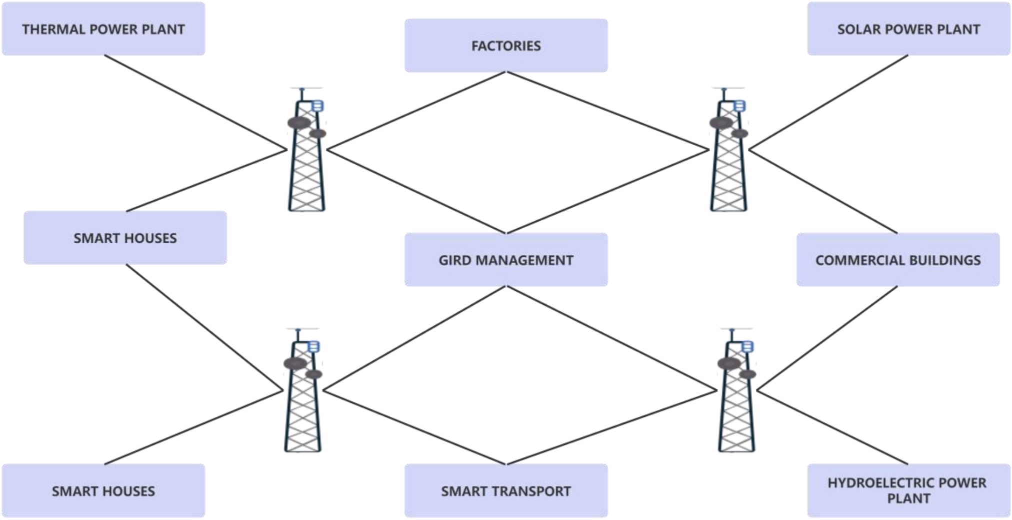


Figure 6. A smart grid conceptual model [32]

Each of the seven domains of the smart grid conceptual model are defined in Table 1.

Table 1. Domains of A Smart Grid Conceptual Model [32]

No.	Domain	Roles/Services in the Domain
1	Customer	End consumers of electricity. May also produce, store, and control energy consumption. Residential, commercial, and industrial customers are included and each of them has its own subdomain.
2	Markets	Facilitators and players in power markets along with other economic processes utilised to maximise system results.
3	Service Provider	The organisations that provide services to utilities and electricity users.

4	Operations	Administrators of the flow of electricity.
5	Generation (including DER)	The electricity's generators. Also capable of storing energy for later use. Traditional generating sources and dispersed energy resources comprise this domain (DER). On a logical level, "generation" encompasses conventional thermal power, hydro power generation, and utility-scale renewable installations that are typically coupled to the transmission system. DER is related with customer- and distributed generations, storage, and demand response, as well as service provider-aggregated energy resources.
6	Transmission	Long-distance electrical conductors that transport high-voltage electricity. Also capable of storing and producing power.
7	Distribution	The entities that transmit and receive electricity for clients. Also capable of storing and producing power.

3.2 Substation Automation System

With the advancement of computer and network technology, and in response to the demands of industry growth, the electric power industry is fiercely promoting the integration and centralised administration of the industrial control system itself, and the smart grid will follow. The automation of substations in power generating systems is a crucial step in the implementation of smart grid technologies as modern electrical or digital information and communication technologies [7]. As a vital component of the smart grid, the substation is responsible for duties such as voltage conversion, power distribution, and the administration and control of power transmission and distribution. To maintain the safe and dependable functioning of the whole energy network, it is necessary to ensure the security of smart substations.

Owing to its significance, the smart substation is connected to the whole power supply in a certain region. Nowadays, there are also many malicious assaults on smart substations by attackers with ulterior objectives, posing grave threats to the security of smart substations and potentially paralysing the whole power system, resulting in substantial economic losses, for example, the 2019 blackout in Venezuela. Once a little fault happens in a particular functional module of the intelligent substation, the corresponding loss will be unquantifiable.

Realising the automation of substations in the power distribution system is a crucial step in putting smart grid technology into practice as a contemporary electrical or digital information and communication technology [7]. To ensure the normal and steady functioning of the power system, it is essential to ensure the security of smart substations.

3.2.1 IEC61850

International Electrotechnical Commission endorsed IEC61850 in 2003 as a substation communication standard based on Ethernet [33]. As a relatively recent international standard, IEC61850 describes substation and equipment information using an object-oriented approach and a unified modelling language by defining logical devices, logical nodes, data objects, data attributes, and common data types [34][35]. The IEC61850 standard is anticipated to enable and assure smooth communication and integration of IEDs from different manufacturers into a hierarchical structure. Simultaneously, individuals anticipate developing an object-based data model, allowing the model to self-describe.

The following are features of the IEC61850 Communication Protocol System [35][36][37]:

- Information hierarchy of the SAS

The SAS communication network and system protocol IEC61850 standard draught presented the notion of data layering in the substation, split the communication system of the substation into three levels, namely the substation level, the interval level and the process level. The following figure is the structure of IEC61850.

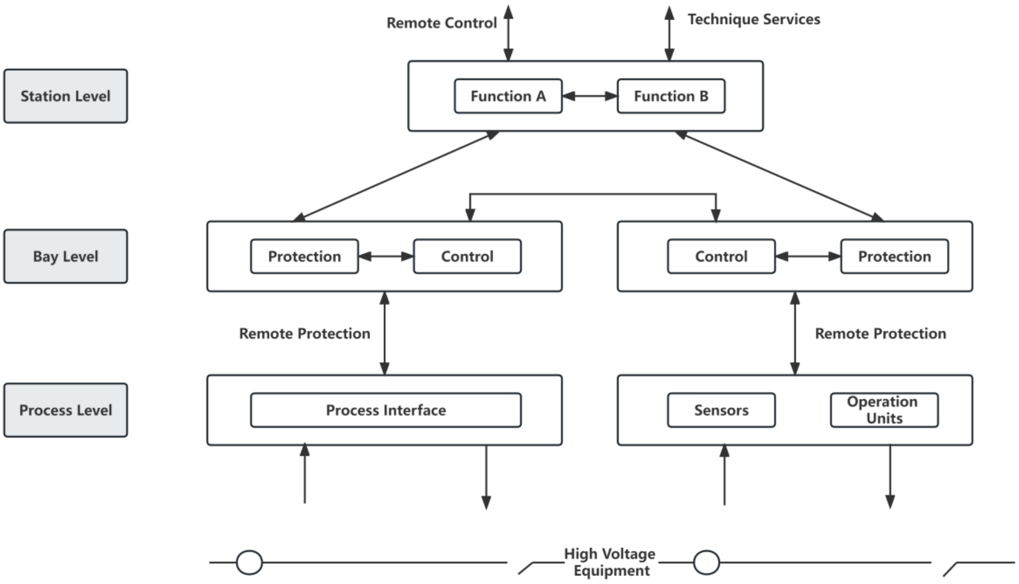


Figure 7. The structure of the IEC61850 [35-37]

- Object-oriented data modelling technology

The IEC61850 standard employs object-oriented modelling technology and specifies a data model based on client/server structure.

- Data self-description

This standard describes the naming criteria for constructing item names utilizing gadget names, LN names, example numbers, and data class names; it employs item-oriented techniques to build communication services among items.

- Network independence

The IEC 61850 standard summarises the communication services essential for information transmission in substations, and proposes an abstract communication service interface (ACSI) independent of the network and application layer protocols employed [35-37].

3.2.2 Substation Automation System

Network security is a crucial foundation for ensuring the safety and stability of smart substation operations [38][39][40]. Smart substations capitalize on cutting-edge, dependable, integrated, and eco-friendly smart technologies, prioritise digitization, and automate important tasks such as data collecting, measurement, control, prevention, and detection. In addition, this is a modern substation with advanced features such as real-time automatic grid control, smart adaptation, online analysis and judgement, and collaborative participation.

The smart substation's secondary system has 3 levels and 2 networks. There are the station level, process level, bay level, the station control level and the network for the process level in sequence[40][41][42]. The three levels would be enumerated and explained in detail below [33][40][41][43][44]. The substation construction depending upon IEC61850 is depicted in Figure 8.

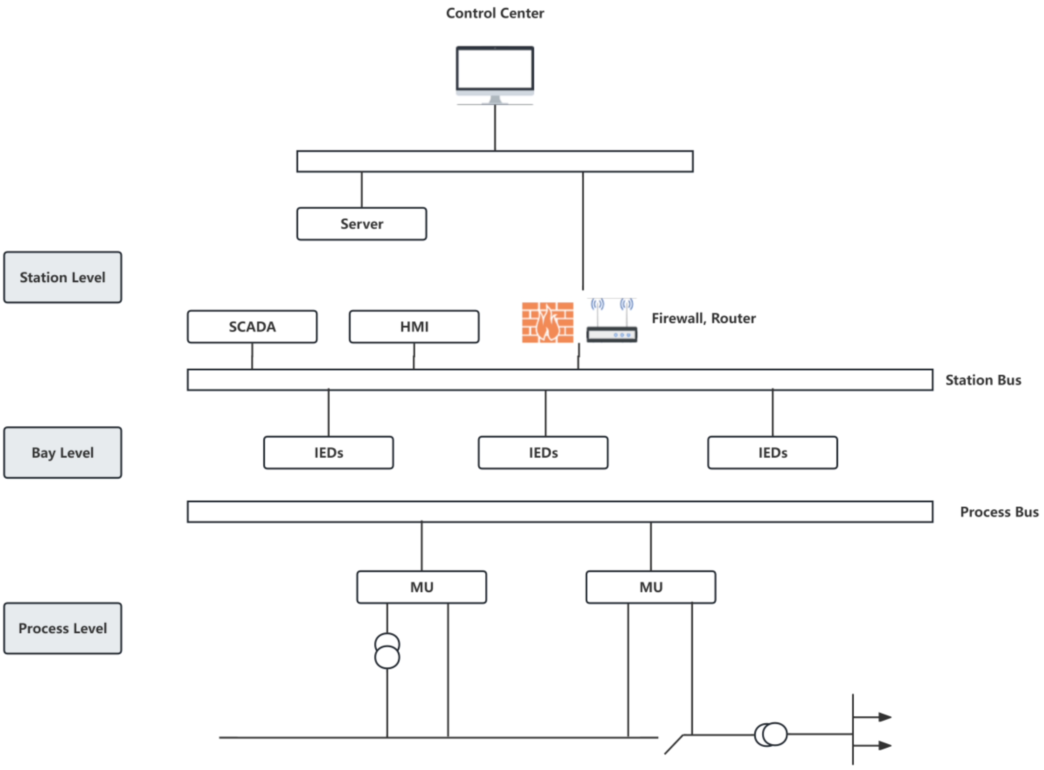


Figure 8. IEC61850-based substation automation system [41][43][44]

- The station level: The station level consists of a host and operator station, a telecontrol communication device, an interprocess communication record analysis system, and numerous secondary functional stations [40-44]. It serves as an interface between human operators and the substation's machinery, enabling the operating personnel to carry out their duties. The layer responsible for overseeing the entire station, including bay level and process level devices, is the station control layer. Its functions include monitoring, control, alarm, and information sharing. Additionally, it is responsible for collecting and managing the associated electrical quantity characteristics, protection signals, and operation information. The intelligent substation's control and monitoring center is responsible for connecting with the distant control center and transmitting all the required data to the control center.

- The bay level: The bay level consists ancillary equipment, including instrumentation for measuring and managing the system, a device for measuring energy consumption, an instrument for protecting against electrical faults, and a device for centralised processing. The spacer device has the capacity to gather data from one interval, influence the operations of the interval's main device, as well as transmit data and control signals via remote ports. A certain amount of autonomy is maintained by the separation layer, which is made up of numerous secondary subsystems. As a result, even in the event of a network connection loss with the station level, the correct operation of the on-site monitoring of the bay level apparatus may be ensured.

- The process level: The process level contains major devices, including transformers, circuit breakers, isolating switches, capacitors and DC power systems, in addition to the accompanying smart units and smart terminals. The development of the process level is the most notable structural difference between conventional and intelligent substations. The process level establishes a connection between the primary and secondary devices through the utilization of smart components, smart terminals, and merging units. Auxiliary equipment is responsible for executing tasks that are associated with the primary equipment. These tasks include gathering and transmitting operational data in real-time, monitoring and managing the operational status of the equipment, and receiving and executing remote control commands.

According to the network transmission of the intelligent substation based on IEC61850, the network from process level to interval level may be classified into GOOSE and SV. GOOSE refers to a type of substation event that is characterized by its object-oriented and generic nature. The main purpose of this technology is to facilitate the exchange of information among multiple IEDs. This includes the sending and receiving of various signals and commands, like tripping and closing, interlocking, and others. Additionally, it boasts a high probability of successful transmission. SV is derived from the publish or subscribe mechanism, the model items and services associated with the sampled value in the sampled data set, and the mapping of model items and services to the ISO/IEC 8802-3 frame.

3.3 Markov Decision Process

Mathematically, The MDP is a discrete-time stochastic control process. It offers a mathematical way to model actions with partially unpredictable and partially controllable results [45]. It is memoryless, meaning that the anticipated state is simply influenced by the current state without any direct relationship to the state in the past [46]. MDPs are useful for analysing optimisation challenges handled by dynamic programming [47]. A MDP is defined as an extension of a Markov Chain (MC) and a Markov Reward Process (MRP), which is a Markov process to which Markov rewards, discounts, and actions have been added.

Figure 9 shows the relationship between MC, MRP and MDP:

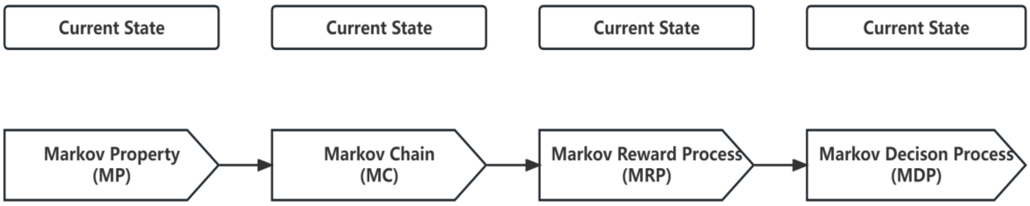


Figure 9. The relationship between MC, MRP and MDP

3.3.1 Markov Process

The MP is a random process with Markov properties, also referred to as the Markov chain.

An MP is defined by:

- A set of states $\mathrm{s} \in S$
- A transition probability P

Typically, an MP is denoted by the tuple $< S, P >$. Assuming there are n states in total, $S = \{s_1, s_2, ..., s_n\}$, the state transition matrix P specifies the probabilities of transition between all possible state pairs [48][49]:

$$P = \begin{bmatrix} P(\mathrm{s}_1|s_1) & \dots & P(s_n|s_1) \\ : & & : \\ P(s_1|s_n) & \dots & P(s_n|s_n) \end{bmatrix}, \tag{1}$$

which represents the probability of the system transitioning to the next state in the current state.

3.3.2 Markov Reward Process

The Markov reward process can be obtained by adding a reward function R and a discount factor γ to the Markov process. It is composed of $< \mathrm{S}, \mathrm{R}, \mathrm{P}, \gamma >$, and the meaning of each component is as follows [50][51].

An MRP is defined by:

- A set of states $\mathrm{s} \in S$
- A reward function R
- A transition probability P
- A discount factor γ

The reward in the current state refers to the reward expectation that can be obtained at the next time $t+1$ in state s at time t.

$$R_s = E[R_{t+1}|S_t = s] \tag{2}$$

- Return

In a Markov reward process, from the state s_t (at the t th moment) to the termination state, the sum of the attenuation of all rewards is called the G_t (Return), the formula is as follows. And R_t means the reward at the t moment.

$$G_t = R_t + \gamma R_{t+1} + \gamma^2 R_{t+2} + ... = \sum_{k=0}^{\infty} \gamma^k R_{t+k} \tag{3}$$

- Value Function

Furthermore, in this process, the expected reward of a state (i.e. the expected future cumulative reward from this state) is called the value of this state. The value of all states constitutes a value function. The input of the value function is a certain state, and the output is the value of this state.

$$\mathrm{V}(s) = E\left[G_t \middle| S_t = s\right] \tag{4}$$

3.3.3 Markov Decision Process

The Markov process and the Markov reward process discussed in Sections 3.3.1 and 3.3.2 both are stochastic processes that change spontaneously. In addition, the Markov decision process (MDP) is derived from the two preceding processes by adding an external "stimulus" to generate and alter the random process. In this model, the attacker's action is considered an external stimulus, and the Markov decision process (MDP) is derived by adding the action to the Markov reward process (MRP).

It is argued that the Markov decision process is a quintuple: (S, A, P, R, γ). The following are components included in it [46][47]:

An MDP is defined by:

- A set of states $s \in S$
- A set of actions $a \in A$
- A transition probability $P(s, s', a)$
- A reward function $R(s, a)$
- A discount factor $\gamma \in (0,1)$
- A terminal state

As shown by the above definition, the state transition probability and reward function of the Markov decision process depend not only on the present state but also on the action taken.

- A action-value function

$$Q(s,a) = E\left[G_t \middle| S_t = s, A_t = a\right], \qquad (5)$$

which represents the expected reward obtained by starting from state s, taking action a, and executing the policy. This function is generally used to measure the value of taking action a in the current state.

- Policy: the distribution of action in a given state,

$$\pi(\mathrm{a}|s) = P[A_t = a|S_t = s] \tag{6}$$

A policy specifies the activities that an attacker may take in various stages, as well as the likelihood that they will perform those actions. The strategy relates solely to the present and has nothing to do with historical data. At the same time, a particular policy is static and unrelated to time; nonetheless, individuals can amend the policy over time. The MDP is a continuous, time-dependent process [47][52]. In general, the interaction process between them is depicted in Figure below: The attacker selects an action based on the current state; the MDP calculates the sum based on the reward function and state transition function, and returns it to the attacker. The objective of an attacker is to maximise the total reward obtained. A policy is a function by which an attacker selects an action from a set of actions based on the current state. Based on Bellman Equation, there are two ways to find the optimal policy: (1) Value iteration, (2) Policy iteration [47].

The specific steps can be seen from the following two flowcharts for value iteration and policy iteration.

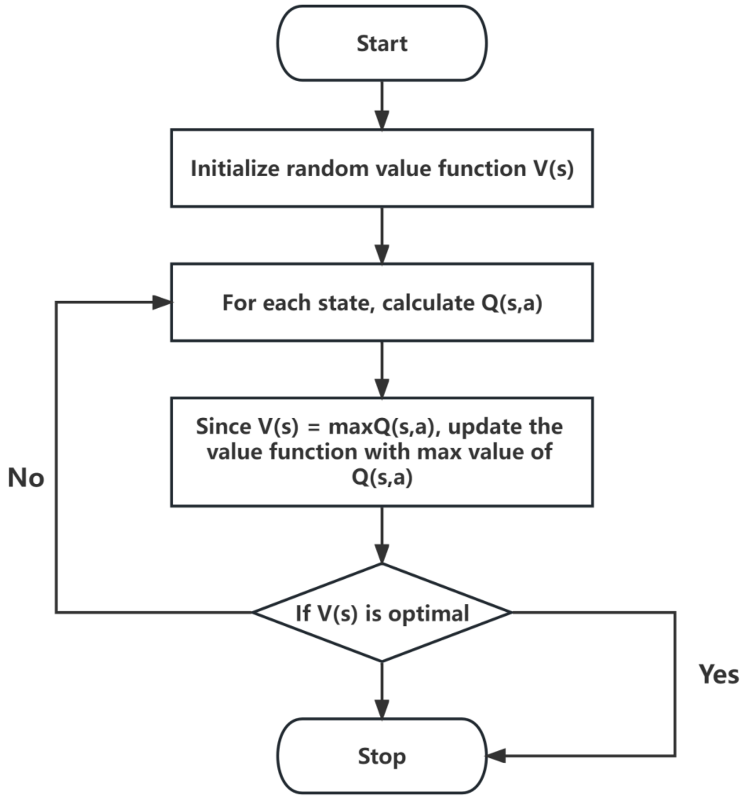

Start
Initialize random value function V(s)
For each state, calculate Q(s,a)
Since V(s) = maxQ(s,a), update the value function with max value of Q(s,a)
No
If V(s) is optimal
Yes
Stop

Figure 10. The flow chart of value iteration [54]

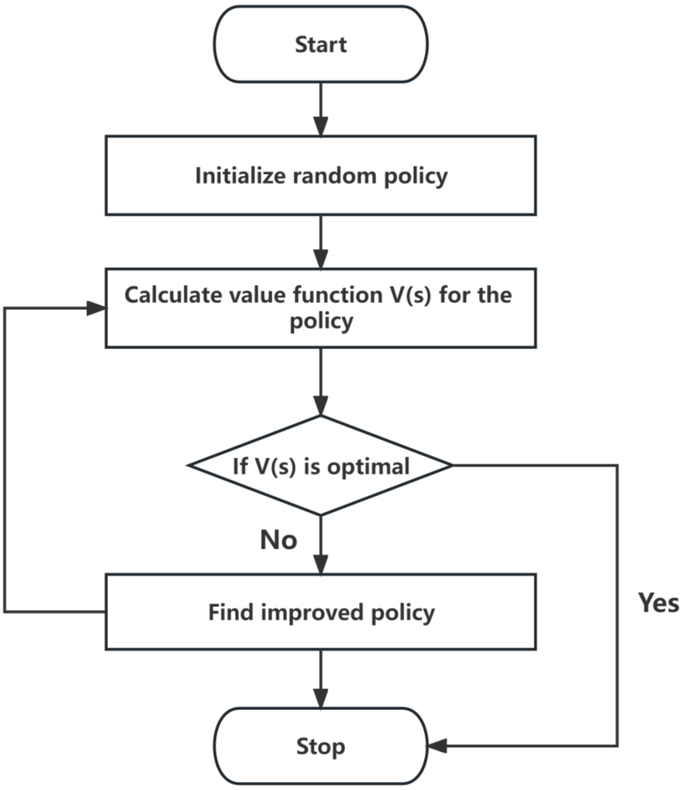


Figure 11. The flow chart of policy iteration [54]

To better illustrate the concept, the following example is based on the MDP.

Consider a 3x2 grid in which the agent may move. Each action can cause the agent to advance one grid to the left, right, up, or down. In each cell, the agent may obtain the following rewards in sequence: +1, -1, -1, +1, +1, -1

The objective of this problem is to maximise the total payout by selecting the optimal action. To tackle this issue, it is operable to construct a policy using the MDP.

- States:

For this 3x2 grid, the states of each cell are represented sequentially using numbers. Therefore, the state space is $\{s_0, s_1, s_2, s_3, s_4, s_5\}$.

- Actions: $\{up, down, left, right\}$
- Probabilities:

Assuming the outcomes of actions are deterministic. This means that for each state-action pair, the agent will move to the neighboring state in the expected direction. For instance, taking a right action in s_0 will transition the agent to s_1, and taking a left action in s_5 will transition the agent to s_4. Therefore, the transition probability can be represented as $P(s, s', a) = 1$, indicating that the probability of transitioning from state s to state s' after taking action a is 1, otherwise it is 0.

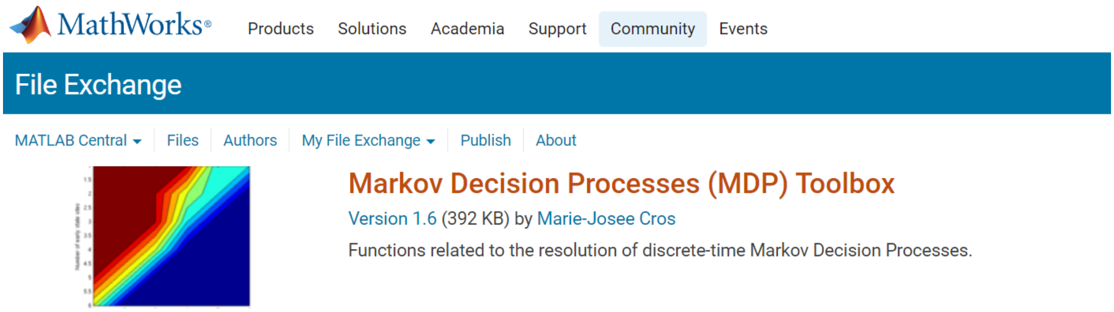
- Rewards: $[+1, -1, -1, +1, +1, -1]$

Based on the defined content above, the MDP can be constructed to model and solve this problem. Various value iteration or policy iteration methods can be used to compute the optimal policy and state-value function, aiming to achieve the objective of obtaining maximum cumulative rewards in a given environment. This dissertation would utilize MATLAB software to perform operations on such problems.

In order to facilitate understanding and lay the groundwork for the following sections, the relevant steps for solving using MATLAB will be detailed here.

- Download the MDP Toolbox for Markov Decision Processes.

(i) Search for the relevant web page and download the toolbox from the page. Figure 12 below is the corresponding interface.



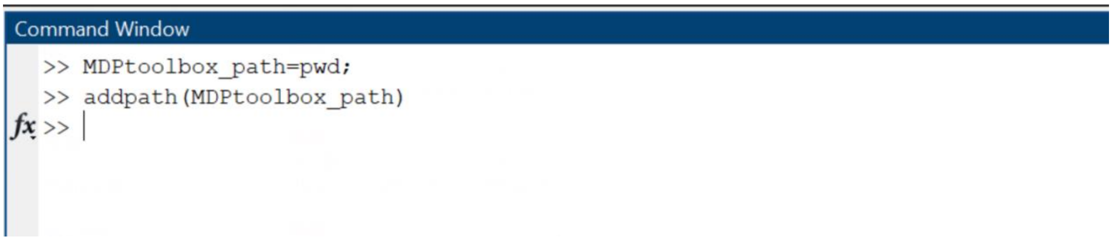
Markov Decision Processes (MDP) Toolbox

Version 1.6 (392 KB) by Marie-Josee Cros

Functions related to the resolution of discrete-time Markov Decision Processes.

Figure 12. The Website of the MDP Toolbox

(ii) Load the toolbox by entering "MDPtoolbox path=pwd;" and "addpath (MDPtoolbox path)" in the Command Window after launching MATLAB. Figure 13 is the corresponding interface.



```
>> MDPtoolbox_path=pwd;
>> addpath(MDPtoolbox_path)
>>
```

Figure 13. The Interface of Loading Up MDP Toolbox

In MATLAB,

- Define the state and action spaces, as well as the probabilities of transitions and rewards. Build an MDP structure including all required information. The transition probability matrix, reward matrix and related codes are shown.

In real implementations, the method may require some fine-tuning in order to reach optimal exploration and exploitation results.

4. Cybersecurity Risk Assessment

4.1 Analysis of Security Attack Based on Substation

The substation is an essential component and pillar of the smart grid [53]. Substations play a crucial role in the transmission and distribution of energy and are outfitted with essential functions to maintain the grid's integrity. Incorporating information and communication technology (ICT) into substations allows smart grid automation functionalities. Nonetheless, the digitalisation of substations is hampered by interoperability concerns between equipment from several vendors. Therefore, the IEC 61850 standard was proposed for digital substation communication between various components [23]. The standard contains a variety of protocols, including Manufacturing Message Specification (MMS), Sampled Value (SV), and Generic Object-Oriented Substation Events (GOOSE) [34].

Although IEC61850 allows for flexibility and real-time communication in digital substations, it has several security vulnerabilities.

Substations automation system based on IEC61850 is susceptible to a variety of cyber threats. It includes not only the ICT-based computer network facilities, but also the physical system facilities of the power grid’s primary and secondary systems. As a result, the purpose of this research is to develop a model that is based on the Markov decision process and will be used to perform network assaults on the substation automation system using a variety of different routes or approaches. As a reference for substation attack decision-making modelling, this research selects seven relatively frequent attack approaches. The precise categories and definitions of these attacks have been described in Chapter 2.1. On the basis of the smart substation's security attack analysis, the risk degree analysis and rating of the seven attack techniques would be performed below.

- High-risk Attack:

(i) DDoS (Distributed Denial of Service): The goal of a DDoS attack is to send a high number of requests to the server in a short period of time in order to overload it and render it inoperable, resulting in system failure or network congestion. This is a particularly dangerous attack on a smart substation, as it could result in device damage, data loss, or substation shutdown.

(ii) FDIA (Fake Data Injection Attack) is a technique for targeting data quality and system integrity by inserting erroneous data into the system. This is a particularly risky method for substation, as it may result in grid problems, improper control decisions, and grid mistakes.

- Middle-risk Attack:

(i) Phishing (Internet Fishing Attack): A Phishing attack is a method of attacking the victim in order to confuse the victim by deceiving them (such as login credentials). This may result in the attacker obtaining the victim's authorization and causing damage to the smart substation.

(ii) Relay Attack: A relay attack deceives victims and obtains sensitive information by assuming the identity of a middleman. This may prompt the attacker to obtain the victim's permissions and launch an attack against the smart substation.

- Low-risk Attack:

(i) MITM (Intermediate Person Attack): A MITM attack involves placing the attacker’s device between the victim and the server in order to intercept or manipulate communication. This may result in some data leakage, but it is unlikely to have a significant effect on the smart substation.

(ii) Malformed Packet: This attack method uses defects or design flaws to deliver a faulty network data packet to a device in order to compromise its functionality. Although this may have some effect on the smart substation, it often has little to no effect on the device's overall security.

(iii) Modification (Data Tampering Attack): This attack method involves the attacker's data being taken and altered by another user. Although this may impact the smart substation's data integrity, it often does not constitute a significant danger to the device's overall security.

The following table 2 classifies the seven attack methods according to the severity of their attacks:

Table 2. Different Types of Cyber Attack Severity Rankings

Type of Attack	Attack class	Description
DDos	1	Distributed denial of service (eg: jamming)
FDIA	2	False data injection attack
Phishing	3	An attempt to steal sensitive information
Relay Attack	4	Re-transmission of old messages
MITM	5	Communication between the IED and SCADA is redirected to a malicious laptop by an attacker at the substation level
Malformed Packet	6	Transmits malformed packets to IEDs
Modification	7	Adulteration of specific attributes

According to Figure 8 in Section 3.2.2, five important attackable components have been selected for modelling in this research. It will sequentially follow the five critical attack components in the intelligent substation. the severity of the damage caused by the attack according to the importance is estimated as follows:

(i) Control Centre: The smart substation's essential component, the control centre is in charge of monitoring and controlling the operation of the entire substation. If the control centre is assaulted, the entire substation's functioning may become out of control, causing the system to collapse or cease and having disastrous repercussions.

The control centre is therefore extremely vulnerable to attack, and its severity is first.

(ii) SCADA & HMI (Monitoring and Human-machine Interface System): The SCADA & HMI system is a crucial system for monitoring and controlling substation components. If it is assaulted, it may result in severe consequences, such as control system damage or system failure. Hence, the SCADA & HMI system is extremely dangerous, and its severity is ranked second.

(iii) IEDs (Intelligent Electronic Devices): An IED is an intelligent electronic device that governs the operation of each subsystem in a smart substation. Attacks on IEDs could result in device malfunction, a halt, or data loss. Nonetheless, compared to the control centre and the SCADA & HMI system, IED danger is relatively low, and its severity ranks third.

(iv) Router/Firewall: Both router and Firewall are essential systems for defending intelligent substations against external threats. They are able to detect and stop harmful traffic. If the router and firewall are compromised, the substation could be subject to a network attack and data leakage. Nonetheless, in comparison to the control centre, SCADA & HMI, and IEDs, the danger associated with the router and firewalls is quite minimal, placing them in fourth place.

(v) MUs (Measurement Units): The measurement unit is crucial equipment for monitoring power demands and grid status. If MU is attacked, it may result in misunderstandings and data inaccuracies, although compared to the other four components stated previously, MU has the lowest risk of assault and the lowest severity ranking.

The following Table 3 evaluates potential attack areas in substations automation system according to their significance:

Table 3. Attackable Components and Value Ranking

Name	Value Ranking
Control Centre	1
SCADA&HMI	2
IEDs	3
Router/Firewall	4
MUs	5

4.2 Analysis of Attack Actions

Due to the significance of the energy system and the potential for major societal and economic losses resulting from cyber assaults, this research primarily uses Markov decision process models. Furthermore, it analyses the network attack and the potential impact of assaulting the smart substation in the smart grid. The following context will combine the comprehensive explanation of the Markov decision process in Chapter 3.3, as well as the previous selection of each attack technique and attacked component. On that basis, the author uses this as a reference for substation attack modelling. Firstly, based on the severity ranking of the seven attack methods examined above and the importance of the five attackable sections, the success likelihood of each component of the smart substation in the face of each attack can be analysed, and a certain degree of assumption can be made.

The preceding assumptions and analysis serve as the foundation for the subsequent modelling of the Markov decision process. Figure 14 depicts the Markov decision process based smart substation network attack model:

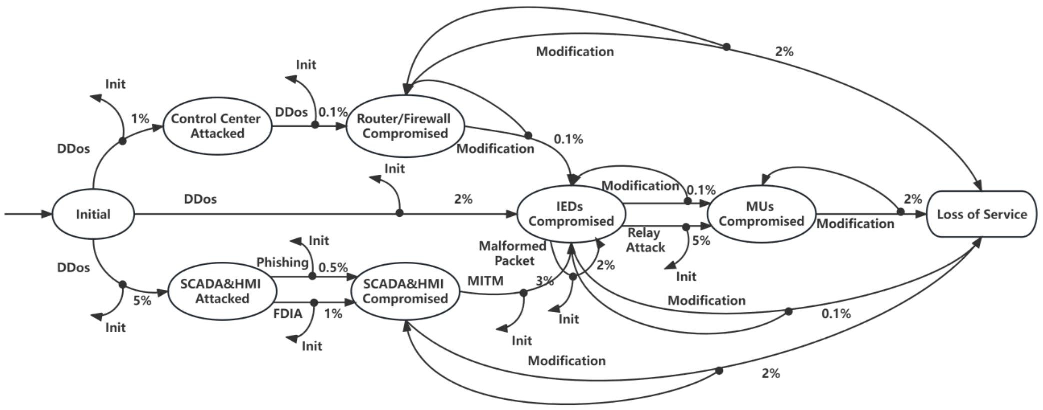


Figure 14. The MDP Model of SAS Attack

The eight circles in this model reflect the attacker's attack location and the eight states: Initial, Control centre attacked, Router/Firewall compromised, SCADA&HMI attacked, SCADA&HMI compromised, IEDs compromised, MUs compromised, and loss of service. "Initial" is an initial state. To simplify the model, this state has two meanings, namely attack start and normal operation. "Loss of Service" is a terminal state, that is, the attack is over, or the attack is successful. The termination state can also be understood as transferring to itself with a 100% probability, so once entered, it stays here.

To simplify the model in Figure 14, the eight states and seven actions are be numbered sequentially, thus constructing a model diagram that is clearer. Figure 15 depicts the simplified MDP model diagram without excessive texts.

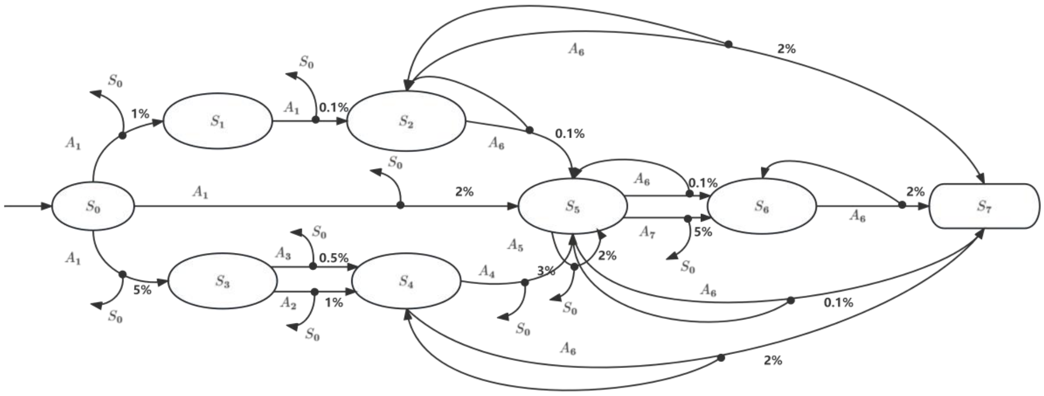


Figure 15. The Simplified MDP Model of the SAS Attack

Take an example to illustrate the above diagram. When the attacker is in the "IEDs compromised" (s_5) state, there is a 5.1% chance of entering the "MUs compromised" (s_6) state; a 2% chance of returning to its own state via "malformed packet attack"; and a 0.1% chance of directly entering the "Loss of service" (s_7) state, indicating the attack is successful.

Suppose the Markov chain begins at the state "SCADA&HMI compromised" (s_4) and finishes at the state "Loss of service" (s_7). According to the state transition diagram, the process in between can have several alternative outcomes, which are referred to as sample episodes:

$s_4 - s_5 - s_0 - s_1 - s_2 - s_5 - s_6 - s_7$

$s_4 - s_5 - s_0 - s_3 - s_4 - s_7$

$s_4 - s_5 - s_5 - s_7$

$s_4 - s_5 - s_6 - s_7$

$s_4 - s_7$

The MDP model can be converted into an MRP adjustment by merging the transition probability from the same state to the next state. In addition, the transition matrix reveals that the sum of each row is 1, i.e., the sum of the transition probabilities from a particular current state to all subsequent states.

4.3 Definition and Explanation of Elements Based on MDP

When constructing the state transition probability matrix, it is essential to assess all possible combinations of states and actions and to compute the chance of migrating to other states when that action is performed. This can be accomplished by repeatedly traversing each state and action and contemplating potential outcomes. For MDP-based agent modelling, the state transition probability matrix is crucial since it defines the conditions the attacker may meet when performing different actions.

The substation information security attack path model diagram based on MDP, in addition to the transition probability, also contains the three essential model parameters, particularly reward, discount, and policy. Each of these characteristics would be discussed individually below.

The diagram of the SAS attack path model based on MDP, as shown in Figure 15, includes the following three parameters:

- Reward: In the Markov decision process, it indicates the benefits that can be achieved by completing an action in the current state s and progressing to the next instant. In the substation information security attack route model, the reward is the degree of influence on system security after an attacker does a particular action in a particular state, whose value might be positive, negative, or zero. For instance, if the attacker uses the “DDoS attack” and the system is attacked, the reward is negative, but if the attacker fails to attack the system after using this action, the reward is positive. Reward structures can assist attackers in making optimal decisions based on their present condition and actions. Hence, R is the reward that corresponds to the state.

In a real-world , the design of the reward matrix is crucial since it directly influences the best strategy of the MDP model. If the reward matrix contains unjustified incentives or penalties, the model may fail to converge or produce an unreasonable strategy.

Furthermore, according to the relevance analysis and rating of each attackable component in the intelligent substation in Section 4.1, Table 4 implies the attacker's profits from assaulting each component.

Table 4. Rewards at Each State

State	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
Loss (£ million)	0	20	10	10	20	15	5	100

- Discount (Discount Factor): In the Markov decision process, the discount factor is the ratio of the present value of future rewards to the present value of current benefits. The discount factor in this MDP model indicates how important future rewards are to the attacker. If the discount factor is bigger, the attacker is more concerned with future benefits, and if it is smaller, the attacker is more concerned with current rewards. The discount factor typically has a range of values between 0 and 1.

- Policy: The attack method selected by the attacker in each stage is referred to as the policy in the Markov decision process. In this MDP model, strategy refers to the network attack method the attacker selects based on the present state and the anticipated reward when facing a particular condition. The selection of policies will depend on the objectives of the attacker. For instance, if the attacker's objective is to maximise reward, he may take an action that maximises reward in the current state or in the future.

5. Results and Discussions

5.1 Introduction

On the basis of the MDP based smart substation network attack model provided in Section 4.1, it is vital to compute the attacker's income for each round based on the attack strategy used. This is the foundation for determining the ideal course of action for an attacker. When an attacker attempts to launch a network attack against a smart substation, the likelihood of success is dependent on the attack method, attack location, and discount factors.

Detailed procedures are as follows:

(i) Initialize the state value function V with a 0 vector and set k = 0 for the number of updates.

(ii) Calculate, for each state, the optimal action value Q (s, a).

(iii) For each state, update its value function V(s) so that it represents the maximum value of all optimal actions, i.e. V(s) = max(Q(s, a)).

(iv) Stop the repetition if the variation of V is less than a threshold; otherwise, add 1 to k and return to step 2.

(v) Calculate the best policy using the optimal action value, i.e., select the action with the maximum action value in each state.

In this study, the MDP model is solved using MATLAB.

Based on the analysis and modeling in Chapter 4, the MDP model's transition probability matrix can generate a three-dimensional array of size 8x8x7. The state transition probability matrix illustrates the likelihood of an adversary transitioning between states. The state transition probability matrix in the model can be represented by a three-dimensional matrix due to the fact that the attacker has a specific failure probability when attempting an attack. The first dimension denotes the current state, the second dimension denotes the subsequent state, and the third dimension denotes the adopted attack strategy. For instance, when the attacker initiates an attack in the "A_1" mode from the s_0 state, there is a 1% chance of transitioning to the s_1 state (Control Centre Attacked), a 2% chance of transitioning to the s_5 state, and a 5% chance of transitioning to the s_3 state, as shown in Figure 15.

Owing to the complexity of the three-dimensional matrix and improved analysis and interpretation, the A6 attack method has been chosen for full enumeration and presentation. It is argued that heat map techniques can visualize data in a two-dimensional format through color variations, making it widely used for intuitive perception [55]. Therefore, a heat map has been chosen here to represent the probability distribution. The state transition probability matrix and heat map of the attacker in attack mode A6 are displayed below.

$$P\_A_6 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.979 & 0 & 0.001 & 0 & 0.020 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.980 & 0 & 0 & 0.020 \\ 0 & 0 & 0 & 0 & 0 & 0.998 & 0.001 & 0.001 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.980 & 0.020 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (7)$$

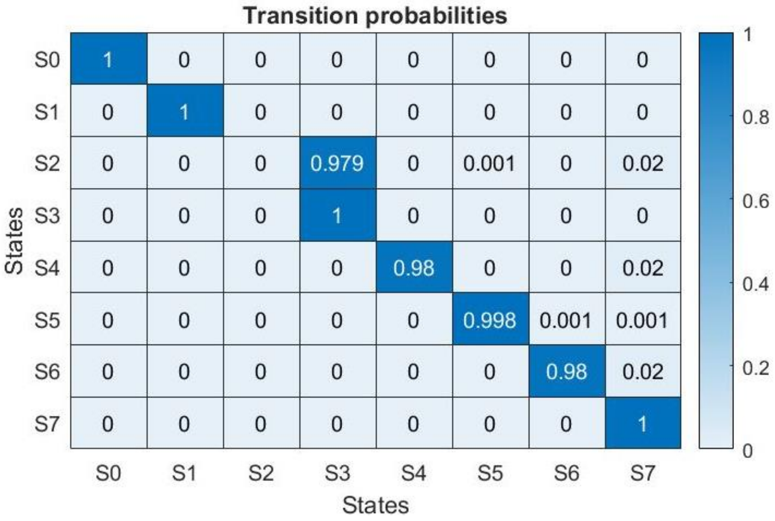


Figure 16. Heatmap of transition probabilities of A6

$$R = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 20 & 0 & 0 & 0 & 0 & 0 & 0 \\ 10 & 0 & 0 & 0 & 0 & 10 & 0 \\ 10 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 20 & 20 & 0 & 0 & 20 & 0 \\ 15 & 0 & 0 & 15 & 15 & 15 & 5 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 100 & 0 \end{bmatrix} \quad (8)$$

As shown above, the reward matrix is a S×A matrix, where S indicates the number of states and A represents the number of actions, as described previously. In this MDP model, there are eight states and seven actions, hence the reward matrix's dimensions are 8 by 7.

The reward matrix describes the immediate compensation for each action in each state. In this paradigm, the attacker performs distinct activities in each state to obtain the relevant reward value. If the attacker successfully employs the attack method in this condition, the associated reward value can be received. For invalid acts, award them with zero. If attackers take the "A4" action in the S4 state and the attack succeeds, they will receive +15 reward value. In contrast, if they takes the "A2" action in the S3 state, the reward will be 0 if the attack fails, since the system is operating correctly and attackers' activity did not cause any damage to the system. The goal of establishing the corresponding reward value is to demonstrate that the attacker intends to successfully attack and affect the system as quickly as possible, while preventing it from getting into a state and performing the same behaviour repeatedly.

In addition, the discount factor determines the importance of future rewards relative to immediate rewards. Typically, the discount factor takes a value between 0 and 1. The specific value needs to be chosen based on the characteristics and goals of the problem. In this model, based on the requirements of this article and combined with the analysis mentioned earlier, the 0.95, 0.90, 0.75, 0.5, and 0.2 discount factors would be assumed and selected for evaluation in the following section.

5.2 Results

In 5.1, a series of analysis determined the network attack path of the smart substation in the energy network was presented. Without proper reconnaissance and other preliminary measures, it is challenging for attackers to comprehend the internal structure and prospective attack vectors of substations in detail. After executing the initial assault, the assailant will possess the relevant attack targets and hints. At this stage, the attacker can select whether to return to the initial attack state or undertake a meaningful attack by utilising known hints and knowledge. Taking into account the limitations of behaviour, the default attacker will make every effort to attack and reap the greatest possible profit during the process of solution.

MATLAB's MDP toolbox function is used to determine the policy based on the model constructed in Chapter 4.2 and the parameters defined in Chapter 4.3. Through the analysis and solution procedures in Chapter 5.1. Figure 17 displays the policy selection process.

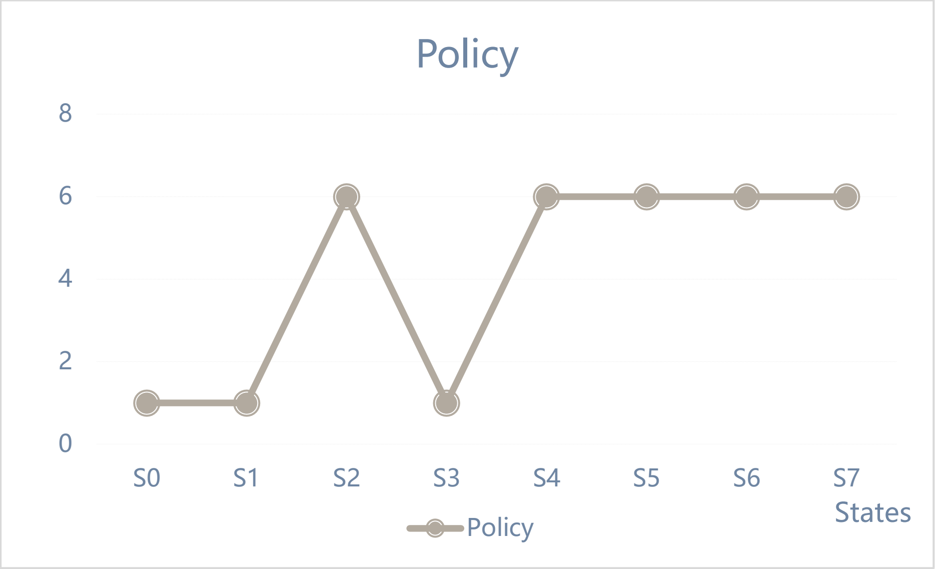


Figure 17. The policy selections

Depending on the outcome of the strategy, cumulative returns can vary, and these returns can be used to evaluate the quality of the approach. Hence, the following will examine the benefits and drawbacks of various tactics by comparing their outcomes and select the most effective strategy for solving real problems. Figure 18 below is the line chart about the Value when the discount factor is 0.95.

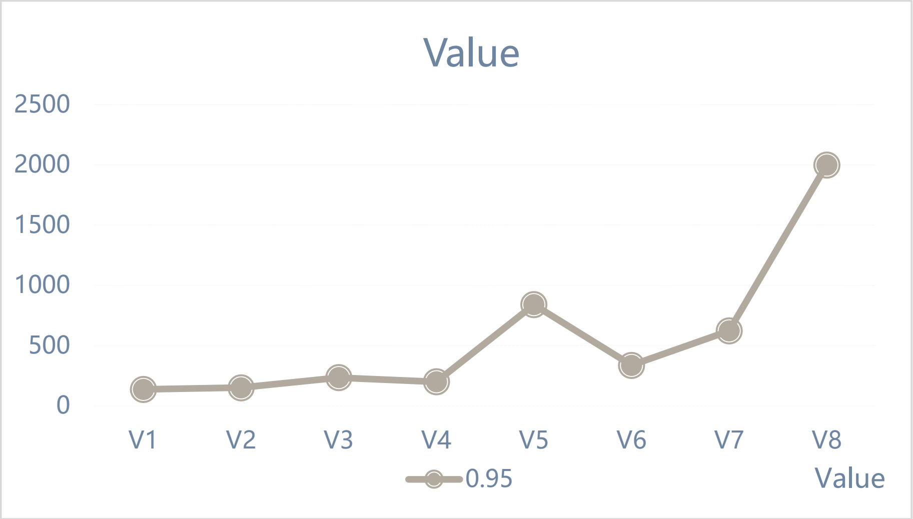


Figure 18. The value when the discount factor is 0.95

As shown in Figure 18, when the attacker's assault path reaches the termination state s_7, the attack gain is at its highest, i.e., the damage to the smart substation in the energy network is at its worst. In addition, while the attacker is in state s_4, the attack income is about one billion pounds, causing significant system damage.

Figure 19 provides information regarding different values when the discount factors are 0.7, 0.9, and 0.95. In addition, Figure 20 illustrates the return value's trend of change when the discount factor is 0.5 and 0.2.

It is clear that although the selection of the discount factor differs, it has no impact on the policy selection. Also, the discount factors and the return values remain the similar trend in the entire given period. The return value increases with the growth of discount factor.

Specifically, the reward increases steadily from 1.83 to a peak of about 20 billion pounds when the discount is 0.95. Similarly, reward values grow gradually under other discount factors.

On the other hand, it can be observed from these numbers that the attacker must enter terminal state s_7 in order to obtain the highest success. Excluding the terminated state, the state s_4 (SCADA and HMI Compromised) attack path generated the most incredible damage. In addition, the loss caused by the attacker gradually diminishes for states s_5, s_2, and s_3.

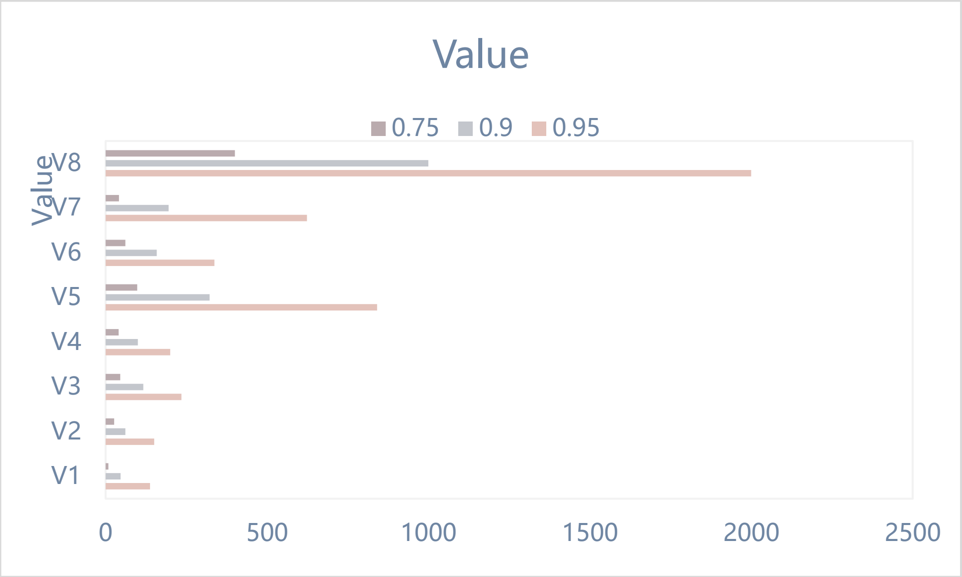


Figure 19. The values when the discount factors are 0.7, 0.9 and 0.95

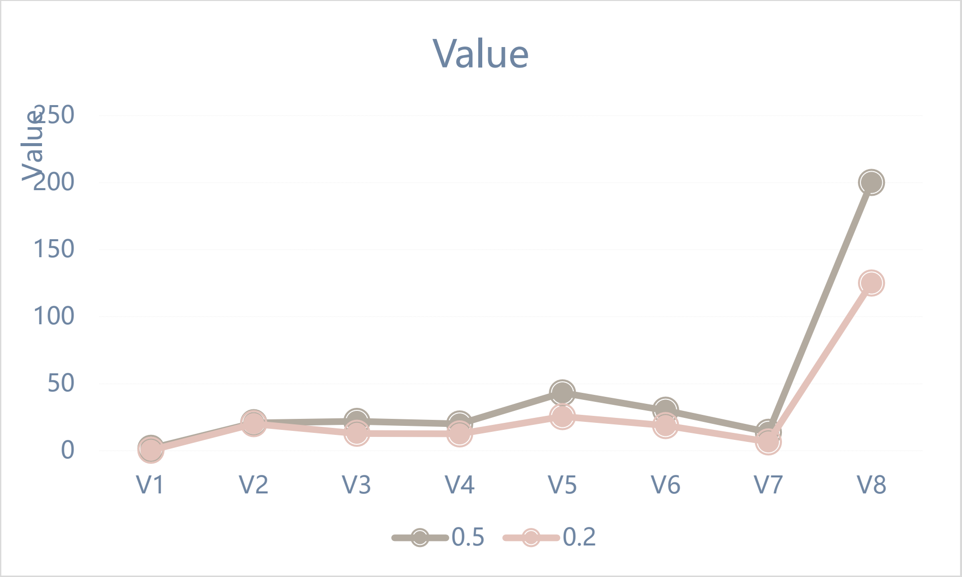


Figure 20. The values when the discount factors are 0.5 and 0.2

5.3 Analysis

The discount factor is a parameter used in MDPs to balance the link between long-term and short-term incentives. The discount factor can take on values between 0 and 1. When assaulting, attackers will weigh not only future rewards, but also the value of immediate rewards. In this MDP model, it is assumed that the discount factors have respective values of 0.95, 0.90, 0.75, 0.5 and 0.2.

If the discount factor is set to a number near 0, such as 0.20, the attacker may neglect to explore remote areas, which may cost several steps to reach and provide no instant benefits. In contrast, if the discount factor is set to a number near 1, such as 0.95, the attacker may be more motivated to engage in long-term planning and perhaps conduct riskier activities in pursuit of bigger long-term gains. However, when the discount factor is close to 1, it may increase the computing complexity of the MDP issue since a longer accumulation time of rewards must be accounted for.

If the attacker is to be successful, the discount factor's value must be chosen based on the individual situation. The significance of balancing long-term and short-term benefits, as well as the computing complexity should be taken into account.

In addition, based on the reward value determined in previous chapters, it is obvious that if an attacker successfully conducts a network attack against a smart substation, it will surely result in substantial losses. In addition, to lessen the strain on defenders, the attack return value derived using this MDP model can infer the attacker's primary assault sites and objectives.

Therefore, it is crucial to understand the significance of each component of the intelligent substation and the implementation of basic defences. The attack path that targets SCADA&HMI components will be relatively favoured by attackers, according to past analysis and solution outcomes. These components, which include IEDs, the Control Centre, etc., can be subject to crucial monitoring and protection measures.

Depending on the attack type, attack location, and attack path chosen, various defence strategies are typically employed. Below is a list of defence strategies relating to the MDP model described in this article.

Control Centre, Router/Firewall, SCADA&HMI, IEDs, and MUs are the five most vulnerable components of a smart substation, as determined by the analysis presented in Chapter 4.1. In response to attacks on these areas, the following countermeasures can be implemented:

(1) Control Centre: The control centre is the nerve centre of the smart substation and is responsible for monitoring and controlling the substation's numerous

components. To prevent assaults against the control centre, the following precautions might be taken:

Ensure that the control centre is only accessible via a secure network, thereby restricting external access.

- Install an intrusion detection system and antivirus software to prevent malware from infecting the control centre.
- Regularly back up data so that it can be restored quickly in the case of an attack or data loss.

(2) Router/Firewall : Both of them defend the smart substation network from external assaults. To prevent attacks against routers and firewalls, the following precautions can be taken:

- Set robust passwords and access control lists to restrict router and firewall access.
- Update the software and firmware of routers and firewalls frequently to maintain security.
- Deploy a network intrusion detection system to prevent and monitor illegal network access and attacks.

(1) SCADA and HMI (Supervisory Control and Data Acquisition and Human Machine Interface) are the operating interfaces of the smart substation, indicating

the status of the substation to the operator and regulating its operation. To prevent assaults on SCADA and HMI systems, the following steps can be taken:

- Access to SCADA and HMI systems can be restricted by configuring access control lists and strong passwords.
- Protect SCADA and HMI systems from malware and illegal access by installing anti-virus software and an intrusion detection system.
- Check the logs of SCADA and HMI systems on a regular basis to detect and resolve potential security issues in a timely manner.

(2) IEDs (Intelligent Electronic Devices): IEDs are the fundamental equipment of a smart substation, responsible for monitoring and managing the operation of the substation's different components. To prevent attacks on IEDs, the following precautions might be taken:

- To limit access to IEDs, configure robust passwords and access control lists.
- IEDs' firmware and software can be often updated to ensure their security.
- To safeguard IEDs from malware and unauthorized access, install anti-disease safeguard software and intrusion detection systems.

(5) MUs (Measurement Units): MUs are used to monitor the state and operation of the power grid in smart substations. To prevent attacks against MUs, the following measures might be taken:

- Set robust passwords and access control lists to limit MU access.

- The firmware and software of MUs can be updated frequently to ensure their security.
- Protect MUs from malware and unauthorized access by installing anti-virus software and an intrusion detection system.

To ensure the security of smart substations, additional security measures, such as employing security protocols, encrypting communication, restricting network access, etc., can be implemented. Likewise, regular security vulnerability screening and security evaluation are also essential.

6. Conclusions & Future Work

6.1 Conclusions

This research provides an MDP-based modelling method for smart substation network attacks, taking into account the adaptability of smart substations to network attacks and the significance of the safe and stable functioning of energy networks under network threats. For the critical components of a smart substation, the model system is able to perform the required functions and calculate the attack probability and the loss resulting from a successful network attack using several prevalent network attack methods.

This thesis mostly has accomplished the following:

(1) The common security threats and techniques of attack in the energy network have been evaluated. In addition, the significance of intelligent networks and the need to protect their data have been underlined.

(2) The author has discovered suitable modelling and problem-solving theories and techniques, and established the overall tone of the text by analysing and learning from prevalent network security risk assessment approaches.

(3) The MDP that is ideal for tackling dynamic programming issues has been selected in terms of modeling, and the MDP has been explained and analysed in detail.

(4) For the information security of energy substations, seven common attack methods have been listed and used, namely DDos attack, FDIA, phishing, relay attack, MITM, malformed packet attack and modification.

(5) Based on deeply analysis of the characteristics of SAS, five key parts have been selected, namely Control Centre, SCADA&HMI, IEDs, Router/Firewall and MUs.

(6) The probability of successful attacks by several network attack paths has been studied. In addition, the MDP model's parameters have been set and solved in detail.

(7) The effectiveness and the validity of the model have been demonstrated by discussing and attempting to synthesize the attack return values of various discounted variables in this thesis.

6.2 Future Work

This research provides a new MDP_based network security risk assessment methodology and calculation approach for the smart substation network attack model. In addition, it can examine the potential losses caused by network threats and the substation components that need to be secured based on the solution's values. Furthermore, the smart substation is a crucial component of the energy network, and the study of its network security contributes to the investigation of information security in the energy network.

Although the aims and objectives mentioned before have been accomplished, the risk of network assaults based on smart substations can be now analysed and calculated. There are still parts of research that can be further improved. Due to the limited time, the performed research did not include hardware aspects, meaning that further research can be done on practical experiments with necessary equipment. Currently, analytic model of MDP in MATLAB has been explored and satisfactory outcomes have been produced, however, the model can still be enhanced. Based on the author’s conducted research, the following aspects should be investigated in the future.

(1) More impact factors, such as defence equipment, human intervention and attack cost can be introduced into the model to enhance its performance.

(2) State transition probability should be further researched in the aspect of hardware. Owing to the limited literature on this part, experiments with necessary equipment can be used to obtain a more realistic value for the probability.

(3) Defender's protections might be incorporated later to further optimize the model. In this thesis, only the cyber attack components were considered. However, the digital substation in the energy network is a complex and dynamic system, and substation personnel will take defensive measures in addition to the attacker's attack in the real world.

With the advancement of technology, the energy network has become progressively more diversified and intricate, posing significant obstacles to its safe and stable functioning. In a complicated network security environment, the energy network's infrastructure poses a certain level of network security risk. The severity of the network risks facing the electricity sector is increasing. These network risks may not only pose a significant risk to individual privacy, but also result in significant social losses. In order to ensure the information security of the energy network, it is imperative to do an additional in-depth study, which has significant societal implications.

References

[1] “UK enshrines New Target in law to slash emissions by 78% by 2035,” GOV.UK, https://www.gov.uk/government/news/uk-enshrines-new-target-in-law-to-slash-emissions-by-78-by-2035 (accessed May 15, 2022).

[2] C. Sun, Z. Mi, and H. Ren, “Sustainability Evaluation in power system related applications — a review,” *2016 IEEE International Conference on Power System Technology (POWERCON)*, 2016. doi:10.1109/powercon.2016.7753901

[3] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber attack-resilient control for smart grid,” *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2012. doi:10.1109/isgt.2012.6175567

[4] Analysis of the cyber attack on the Ukrainian Power Grid, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/03/Documents_E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf (accessed May 15, 2023).

[5] A. Shehod, Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US, https://web.mit.edu/smadnick/www/wp/2016-22.pdf (accessed May 15, 2023).

[6] B. Hyder and M. Govindarasu, "Optimization of cybersecurity investment strategies in the smart grid using game-theory," *2020 IEEE Power &amp; Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2020. doi:10.1109/isgt45199.2020.9087634

[7] Md. S. Ali, A. Sultana, and J. N. Supti, "Enhancing smart grid in Bangladesh Power Distribution System using substation automation," *2015 International Conference on Electrical &amp; Electronic Engineering (ICEEE)*, 2015. doi:10.1109/ceee.2015.7428282

[8] J. Rifkin, *The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World*. New York: St. Martin's Griffin, 2013.

[9] X. Jin, Y. Zhang, and X. Wang, "Strategy and coordinated development of strong and smart grid," *IEEE PES Innovative Smart Grid Technologies*, 2012. doi:10.1109/isgt-asia.2012.6303208

[10] M. Moness and A. M. Moustafa, "A survey of cyber-physical advances and challenges of wind energy conversion systems: Prospects for internet of energy," *IEEE Internet of Things Journal*, vol. 3, no. 2, pp. 134–145, 2016. doi:10.1109/jiot.2015.2478381

[11] C.-K. Tham and T. Luo, "Sensing-driven energy purchasing in smart grid cyber-physical system," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 43, no. 4, pp. 773–784, 2013. doi:10.1109/tsmca.2012.2224337

[12] G. Celli, P. A. Pegoraro, F. Pilo, G. Pisano, and S. Sulis, "DMS cyber-physical simulation for assessing the impact of state estimation and communication media in Smart Grid Operation," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2436–2446, 2014. doi:10.1109/tpwrs.2014.2301639

[13] Modern grid benefits - National Energy Technology Laboratory, https://netl.doe.gov/sites/default/files/Smartgrid/Modern-Grid-Benefits_Final_v1_0.pdf (accessed May 15, 2023).

[14] J. Liu, D. Niu, and X. Song, “The energy supply and demand pattern of China: A review of evolution and sustainable development,” *Renewable and Sustainable Energy Reviews*, vol. 25, pp. 220–228, 2013. doi:10.1016/j.rser.2013.01.061

[15] R. Campbell, The smart grid and cybersecurity -- regulatory policy and issues, https://sgp.fas.org/crs/misc/R41886.pdf (accessed May 15, 2023).

[16] T. Krause, R. Ernst, and B. Klaer, “Cybersecurity in power grids: Challenges and opportunities,” *Sensors*, vol. 21, no. 18, p. 6225, 2021. doi:10.3390/s21186225

[17] F. Dharmesh, S. Vlachou, and O. Kalopoulou, “Cybersecurity in smart grids, challenges and solutions,” *AIMS Electronics and Electrical Engineering*, vol. 5, pp. 24–37, 2021. doi: 10.3934/electreng.2021002

[18] M. Z. Gunduz and R. Das, “Cyber-security on Smart Grid: Threats and potential solutions,” *Computer Networks*, vol. 169, p. 107094, 2020. doi:10.1016/j.comnet.2019.107094

[19] S. Kivalov and I. Strelkovskaya, “Detection and prediction of ddos cyber attacks using spline functions,” *2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2022. doi:10.1109/tcset55632.2022.9766940

[20] What is phishing: Attack Techniques & Scam examples: Imperva, https://www.imperva.com/learn/application-security/phishing-attack-scam/ (accessed May 15, 2023).

[21] What is False Data Injection?, https://crashtest-security.com/false-data-injection-attack/ (accessed May 15, 2023).

[22] Y. Li, D. Li, and W. Cui, “Research based on OSI model,” *2011 IEEE 3rd International Conference on Communication Software and Networks*, 2011. doi:10.1109/iccsn.2011.6014631

[23] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice*. Amsterdam: Elsevier/Syngress, Syngress is a imprint of Elsevier, 2014.

[24] H. Karimipour and V. Dinavahi, “Robust massively parallel dynamic state estimation of power systems against Cyber-Attack,” *IEEE Access*, vol. 6, pp. 2984–2995, 2018. doi:10.1109/access.2017.2786584

[25] A. Vernotte, M. Välja, and M. Korman, “Load balancing of renewable energy: A cyber security analysis,” *Energy Informatics*, vol. 1, no. 1, 2018. doi:10.1186/s42162-018-0010-x

[26] K. Kimani, V. Oduol, and K. Langat, “Cyber security challenges for IOT-based Smart Grid Networks,” *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, 2019. doi:10.1016/j.ijcip.2019.01.001

[27] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, “Cyber security for fog-based smart grid SCADA systems: Solutions and challenges,” *Journal of Information Security and Applications*, vol. 52, p. 102500, 2020. doi:10.1016/j.jisa.2020.102500

[28] M. Ni, A. K. Srivastava, and R. Bo, “Design of a game theory based defense system for Power System Cyber Security,” *2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, 2017. doi:10.1109/cyber.2017.8446449

[29] L. D. Kannberg, D. P. Chassin, and J. G. DeSteese, *The benefits of a transformed energy system*, 2003. doi:10.2172/15010370

[30] A. Azarpour, O. Mohammadzadeh, and N. Rezaei, “Current status and future prospects of renewable and Sustainable Energy in North America: Progress and challenges,” Energy Conversion and Management, vol. 269, p. 115945, 2022. doi:10.1016/j.enconman.2022.115945

[31] “Smart Grid: The smart grid,” The Smart Grid, https://www.smartgrid.gov/the_smart_grid/smart_grid.html (accessed May 15, 2023).

[32] A. Gopstein, C. Nguyen, and C. O’Fallon, *NIST framework and Roadmap for Smart Grid Interoperability Standards, release 4.0*, 2021. doi:10.6028/nist.sp.1108r4

[33] R. Macwan, C. Drew, and P. Panumpabi, “Collaborative defense against data injection attack in IEC61850 based smart substations,” *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 2016. doi:10.1109/pesgm.2016.7741376

[34] T. Kostic, O. Preiss, and C. Frei, “Understanding and using the IEC 61850: A case for meta-modelling,” *Computer Standards &amp; Interfaces*, vol. 27, no. 6, pp. 679–695, 2005. doi:10.1016/j.csi.2004.09.008

[35] Z. Huang, L. Gao, and Y. Yang, “IEC 61850 standards and Configuration Technology,” *IEC 61850-Based Smart Substations,* pp. 25–62, 2019. doi:10.1016/b978-0-12-815158-7.00002-0

[36] W. Huang, “Learn IEC 61850 configuration in 30 minutes,” *2018 71st Annual Conference for Protective Relay Engineers (CPRE),* 2018. doi:10.1109/cpre.2018.8349803

[37] M. C. Janssen, P. A. Crossley, and L. Yang, “Bringing IEC 61850 and Smart Grid together,” *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies,* 2011. doi:10.1109/isgteurope.2011.6162749

[38] J. Hong, R. F. Nuqui, and A. Kondabathini, “Cyber Attack Resilient Distance Protection and circuit breaker control for digital substations,” *IEEE Transactions on Industrial Informatics,* vol. 15, no. 7, pp. 4332–4341, 2019. doi:10.1109/tii.2018.2884728

[39] Y. Kwon, S. Lee, and R. King, “Behavior analysis and anomaly detection for a digital substation on Cyber-Physical System,” *Electronics,* vol. 8, no. 3, p. 326, 2019. doi:10.3390/electronics8030326

[40] J. Li, X. Ding, and H. Liu, “Network Security Protection Method of smart substation based on IEC61850 message encryption and flow detection,” *2022 7th Asia Conference on Power and Electrical Engineering (ACPEE),* 2022. doi:10.1109/acpee53904.2022.9783968

[41] R. Zhu, J. Hong, and C.-C. Liu, “Cyber system recovery for IEC 61850 substations,” *2021 IEEE Power &amp; Energy Society Innovative Smart Grid Technologies Conference (ISGT),* 2021. doi:10.1109/isgt49243.2021.9372195

[42] Q. Huang, “Smart substation: State of the art and future development,” *2018 IEEE Power &amp; Energy Society General Meeting (PESGM),* 2018. doi:10.1109/pesgm.2018.8585942

[43] K. Yashwant and K. S. Swarup, “Modeling an IEC61850 based Substation Automation System,” *2011 Annual IEEE India Conference,* 2011. doi:10.1109/indcon.2011.6139517

[44] O. Duman, M. Zhang, and L. Wang, “Measuring the security posture of IEC 61850 substations with redundancy against Zero Day attacks,” *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm),* 2017. doi:10.1109/smartgridcomm.2017.8340727

[45] L. Zhang, Y. Dong, and D. Nan, “Reliability Analysis of Intelligent Substation Protection System based on Markov Model,” *2020 Chinese Control And Decision Conference (CCDC)*, 2020. doi:10.1109/ccdc49329.2020.9164269

[46] L. M. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. New York etc.: John Wiley & Sons, 2005.

[47] A. Bashar, S. Muhammad, and N. Mohammad, “Modeling and analysis of MDP-based security risk assessment system for smart grids,” *2020 Fourth International Conference on Inventive Systems and Control (ICISC)*, 2020. doi:10.1109/icisc47916.2020.9171072

[48] R. A. Howard, *Dynamic Programming and Markov Processes*. Cambridge, MA: M.I.T. Press, 1972.

[49] B. W. Dickinson, A. Fettweis, and J. L. Massey, *Markov Chains and Stochastic Stability*. London: Springer London, 1993.

[50] R. M. Smith, *Markov Reward Processes: A Final Report*. Washington, DC: National Aeronautics and Space Administration, 1991.

[51] M. K. Smotherman, “Transient solutions of time-inhomogeneous Markov reward models with discontinuous rates,” *Numerical Solution of Markov Chains*, pp. 385–399, 2021. doi:10.1201/9781003210160-20

[52] R. S. Sutton, “Introduction: The Challenge of Reinforcement Learning,” *Reinforcement Learning*, pp. 1–3, 1992. doi:10.1007/978-1-4615-3618-5_1

[53] Z. Wang, K. Zhang, and H. Li, “Evaluation method of substation weak link based on power grid risk severity indexs,” *2021 IEEE 5th Information Technology,Networking,Electronic and Automation Control Conference (ITNEC)*, 2021. doi:10.1109/itnec52019.2021.9586816

[54] Hands-on reinforcement learning with python, https://github.com/PacktPublishing/Hands-On-Reinforcement-Learning-with-Python (accessed May 15, 2023).

[55] S. Singhal, All about heatmaps, https://towardsdatascience.com/all-about-heatmaps-bb7d97f099d7 (accessed May 15, 2023).

Appendix

```
MDPtoolbox_path=pwd;
addpath(MDPtoolbox_path)

% Set transition probability matrix
P(:,:,1) = [
0.92, 0.01, 0, 0.05, 0, 0.02, 0, 0;
0.999, 0, 0.001, 0, 0, 0, 0, 0;
0, 0, 1, 0, 0, 0, 0, 0;
0, 0, 0, 1, 0, 0, 0, 0;
0, 0, 0, 0, 1, 0, 0, 0;
0, 0, 0, 0, 0, 1, 0, 0;
0, 0, 0, 0, 0, 0, 1, 0;
0, 0, 0, 0, 0, 0, 0, 1]; %A1

P(:,:,2) = [
1, 0, 0, 0, 0, 0, 0, 0;
0, 1, 0, 0, 0, 0, 0, 0;
0, 0, 1, 0, 0, 0, 0, 0;
0.99, 0, 0, 0, 0.01, 0, 0, 0;
0, 0, 0, 0, 1, 0, 0, 0;
0, 0, 0, 0, 0, 1, 0, 0;
0, 0, 0, 0, 0, 0, 1, 0;
0, 0, 0, 0, 0, 0, 0, 1]; %A2

P(:,:,3) = [
1, 0, 0, 0, 0, 0, 0, 0;
0, 1, 0, 0, 0, 0, 0, 0;
0, 0, 1, 0, 0, 0, 0, 0;
0.995, 0, 0, 0, 0.005, 0, 0, 0;
0, 0, 0, 0, 1, 0, 0, 0;
0, 0, 0, 0, 0, 1, 0, 0;
0, 0, 0, 0, 0, 0, 1, 0;
0, 0, 0, 0, 0, 0, 0, 1]; %A3

P(:,:,4) = [
1, 0, 0, 0, 0, 0, 0, 0;
0, 1, 0, 0, 0, 0, 0, 0;
0, 0, 1, 0, 0, 0, 0, 0;
0, 0, 0, 1, 0, 0, 0, 0;
0.97, 0, 0, 0, 0, 0.03, 0, 0;
0, 0, 0, 0, 0, 1, 0, 0;
0, 0, 0, 0, 0, 0, 1, 0;
0, 0, 0, 0, 0, 0, 0, 1]; %A4

P(:,:,5) = [
1, 0, 0, 0, 0, 0, 0, 0;
0, 1, 0, 0, 0, 0, 0, 0;
0, 0, 1, 0, 0, 0, 0, 0;
0, 0, 0, 1, 0, 0, 0, 0;
0, 0, 0, 0, 1, 0, 0, 0;
0.98, 0, 0, 0, 0, 0.02, 0, 0;
0, 0, 0, 0, 0, 0, 1, 0;
0, 0, 0, 0, 0, 0, 0, 1]; %A5

P(:,:,6) = [
1, 0, 0, 0, 0, 0, 0, 0;
0, 1, 0, 0, 0, 0, 0, 0;
0, 0, 0, 0.979, 0, 0.001, 0, 0.02;
0, 0, 0, 1, 0, 0, 0, 0;
0, 0, 0, 0, 0.98, 0, 0, 0.02;
0, 0, 0, 0, 0, 0.998, 0.001, 0.001;
0, 0, 0, 0, 0, 0, 0.98, 0.02;
0, 0, 0, 0, 0, 0, 0, 1]; %A6

P(:,:,7) = [
1, 0, 0, 0, 0, 0, 0, 0;
0, 1, 0, 0, 0, 0, 0, 0;
0, 0, 1, 0, 0, 0, 0, 0;
0, 0, 0, 1, 0, 0, 0, 0;
0, 0, 0, 0, 1, 0, 0, 0;
0.95, 0, 0, 0, 0, 0, 0.05, 0;
0, 0, 0, 0, 0, 0, 1, 0;
0, 0, 0, 0, 0, 0, 0, 1]; %A7

R(:,1)=[0;20;10;10;0;15;0;0;];
R(:,2)=[0;0;0;0;20;0;0;0;];
R(:,3)=[0;0;0;0;20;0;0;0;];
R(:,4)=[0;0;0;0;0;15;0;0;];
R(:,5)=[0;0;0;0;0;15;0;0];
R(:,6)=[0;0;10;0;20;15;5;100;];
R(:,7)=[0;0;0;0;0;5;0;0];

Discount=0.95;

% check the validity of the model
% solve
[V,policy]= mdp_policy_iteration(P,R,Discount);

[policy]= mdp_value_iteration(P,R,Discount);
```