INDUSTRIAL PLACEMENT WORK DIARY

Academic Year: 2022/2023

20 February – 11 June 2023

Student's Name: Hanlin Cai

Student ID (MU/FZU): 20122161 / 832002117

Module Code / Name: EE382 (EE388FZ)

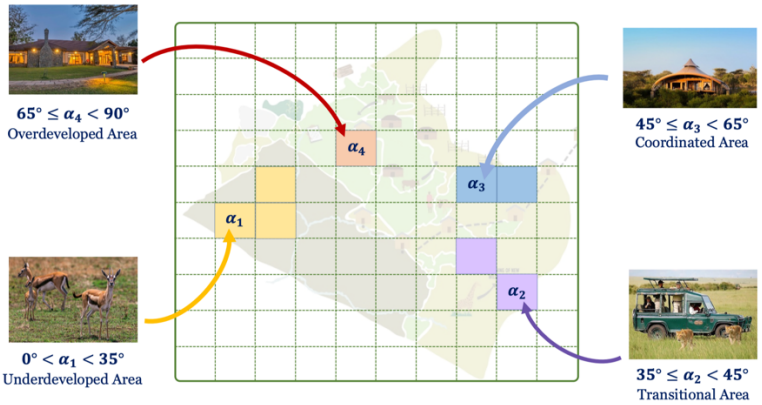
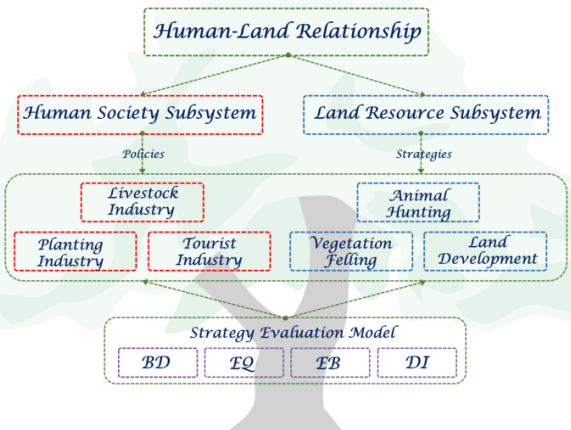
Programme: Robotics and Intelligent Devices

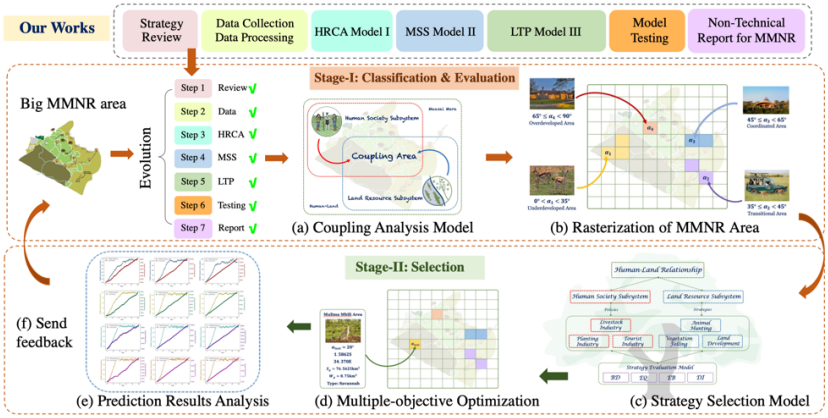
Company & Address: Fujian Huading Intelligent Manufacturing Technology Co. LTD

Building 44, Zone C, Fuzhou Software Park, Software Avenue

Fuzhou City, Fujian Province, China

THE INDUSTRIAL PLACEMENT WORK DIARY MUST BE UPDATED WEEKLY BY THE END OF EACH WEEK IN MOODLE AS A SINGLE DOCUMENT.

Week	Day / Date	Activity / Portfolio
1	Mon 20/2/2023	Supervised by Prof. Zhezhuang Xu, I participate in the Mathematical Contest in Modeling (**MCM** 2023), which is a highly acclaimed contests for international undergraduates. During this competition, I cooperate with Yufei Wu and Wenxuan Luo. Our team once won the First Prize in China Undergraduate Mathematical Contest in Modeling. Besides, the MCM contest lasts for five days. And in the first day, we decided to choose the Topic B (Reimagine Maasai Mara), which is a **discrete problem**. Based on the problem background, we have comprehensively reviewed the related research and resource. Finally, I finished to write the part of **Introduction** and **Literature Review** of our competition paper. For details, our final paper can be accessed here: https://caihanlin.com/mypaper/modeling/202302COMAP.pdf
	Tue 21/2/2023	The MCM Problem B required us to resolve **four objective,** hence we have made a suitable time schedule in advance. On Tuesday, we build our model I (**Human-land Relationship** Coupling Analysis) to address the objective of human-land interaction analysis and area classification. The following Figure 1 illustrates the classification of the Maasai Mara area.  Finally, we suggest six specific strategies for practical implementation.
	Wed 22/2/2023	On Day 3, we firstly propose a four-layer strategy evaluation model based on the **AHP method** to evaluate and rank the policies. The following Figure 2 shows the structure of the strategy evaluation model.  Second, we present the **multi-objective optimization** model to quantify the economic and ecological impact of the optimal combination of the strategies and policies. Finally, we utilized our proposed model to test a representative grid in the MMNR area. The simulation results verify the effectiveness and rationality of our model.

	Thu ***23/2/2023***	On Day 4, considering to resolve the Objective III, we design a long-term trend prediction model to project and assess the long-term ecological and economic situation in the MMNR area based on the optimal management strategies. **First**, we quantify the reflection of trend using the change of animal numbers and resident economic incomes. **Second**, we propose the specific expression of the Logistic Equation, maximum environmental capacity and resident economic incomes. **Third**, based on mathematical definitions, we design a Python program for our trend prediction models. **Finally**, we obtain and present twelve 100-year prediction results referring to twelve different sets of parameter configurations.
	Fri ***24/2/2023***	On the last day, we firstly design a two-page **non-technical report** for the Kenyan Tourism and Wildlife Committee (Objective IV). After finishing the first version of main body, I begin to write the conclusion and summary. Also, I draw a 'fantastic' figure to show the overview of our works, as follows:  Ultimately, I review and polish the whole paper under the guidance of Prof. Xu, and we upload the final manuscript to the COMAP committee.

Summary: In brief, I take part in the 2023 Mathematical Contest in Modeling (MCM) in the first week. Advised by Prof. Xu, we present a paper called Reshape the Crowning Glory of Maasai Mara. Since the MCM contest only lasts for **five days**, it is impossible for our paper to be comprehensive and perfect. Therefore, I plan to further improve and refine our paper in the following weeks. Finally, our final paper can be accessed here: https://caihanlin.com/mypaper/modeling/202302COMAP.pdf

<table>
<tr><th>Week</th><th>Day / Date</th><th>Activity / Portfolio</th></tr>
<tr><td rowspan="3">2</td><td>Mon

27/2/2023</td><td>In this week, we are required to finish the Intern Proposal of Industrial Placement (IP). Therefore, firstly I have a face-to-face talk with my supervisor. And based on the suggestions given by Prof. Xu, I choose the research topic of Exploring Multiple IoT Security Attacks with Machine Learning Based Schemes. Then, I take the most of time to read the related paper. Also, I begin to write the Literature Review of my IP proposal. For details, my IP proposal can be accessed here: https://caihanlin.com/mypaper/IP/Proposal.pdf</td></tr>
<tr><td>Tue
28/2/2023</td><td>In Day 2, I continue to review the existing research works and write the part of Related Literature. Based on the reference, I obtain that many papers have proposed various ML-based methods to prevent specific IoT attacks and improve IoT security. For instance, the Q-learning schemes proposed by Xiao, et al. performed well in the face of both spoofing and jamming attacks. While the SVM schemes proposed by Ozay, et al. could effectively identify and defend against intrusion and spoofing attacks. And the following Table shows the Summary of my reviewing works.
<table>
<tr><th>Attacks</th><th>Security Schemes</th><th>ML Methods</th><th>Performance</th></tr>
<tr><td>Spoofing</td><td>Authentication</td><td>Q-learning[8]</td><td>Average loss rate</td></tr>
<tr><td></td><td>Authentication</td><td>SVM[9]</td><td>Classification accuracy</td></tr>
<tr><td></td><td>Authentication</td><td>DNN[10]</td><td>False alarm rate</td></tr>
<tr><td></td><td>Authentication</td><td>dFW[11]</td><td>Misdetection rate</td></tr>
<tr><td>DoS</td><td>Secure IoT offloading</td><td>MLP[12]</td><td>Detection accuracy</td></tr>
<tr><td></td><td>Access Control</td><td>MCA[13]</td><td>Root mean error</td></tr>
<tr><td></td><td>Flow Detection</td><td>NFS[3]</td><td>Storage efficiency</td></tr>
<tr><td>Intrusion</td><td>Access Control</td><td>Naive Bayes[14]</td><td>False alarm rate</td></tr>
<tr><td></td><td>Access Control</td><td>SVM[9]</td><td>Classification accuracy</td></tr>
<tr><td>Sybil</td><td>Dual Identity</td><td>THC-RPL[4]</td><td>Power consumption</td></tr>
<tr><td>Jamming</td><td>Secure IoT offloading</td><td>Q-learning[8]</td><td>Energy consumption</td></tr>
</table>
Note that my literature exploring is heavily based on the Review Paper published by Xiao, et al in 2020.</td></tr>
<tr><td>Wed

1/3/2022</td><td>As for Day 3, today I have already finished the part of Related Literature, and begin to analyze and compare the methodologies and experimental results between different research. Besides, I write the part of Gap in Existing Knowledge to show the possible improvements we can conduct in the near future.

Through in-deep literature review, I find that most of the solutions proposed by existing studies can address specific security attacks but cannot to define more patterns for detecting dynamic multiple attacks. Therefore, it is feasible for us to design a hybrid defense scheme to resolve this challenge. And it may lead to the potential publication opportunities and positive contributions.</td></tr>
</table>

	Thu ***2/3/2023***	In Day 4, after presenting the gap in existing literature, today I begin to organize the workflow and develop the research schedule. To advance my research scientifically and effectively, I developed a specific research schedule as follows: **Industrial Placement Schedule** Project Lead: Zhezhuang Xu, Hanlin Cai To be honest, I understand the research cannot always proceed smoothly as planned, so I will modify the schedule according to the actual situation.
	Fri ***3/3/2023***	In Day 5, after analysing the research background and existing gaps, in order to address the research problem systematically, I have divided it into the specific research questions listed in the following table. Besides, today I have an online meeting with my supervisor and seniors. Based on the work already done, they give me some useful advice and encourage me to carry out my plan.

WBS	Task	Priority	Resource	Start	Finish	Duration	Done	% Complete
1	In-depth literature review	NORMAL	FZU, Hanlin Cai	Fri 10-Feb-23	Fri 24-Feb-23	12		60%
1.1	Go through the advanced paper	NORMAL	FZU, Hanlin Cai	Fri 10-Feb-23	Tue 21-Feb-23	8		80%
1.2	Repeat the experiments	LOW	FZU, Hanlin Cai	Mon 20-Feb-23	Thu 23-Feb-23	4		60%
1.3	Explore the gaps of existing methods	HIGH	FZU, Hanlin Cai	Fri 24-Feb-23	Fri 24-Feb-23	0		40%
2	Redesign some advanced ML algorithms	NORMAL	FZU, Hanlin Cai	Fri 24-Feb-23	Wed 29-Mar-23	24		20%
3	Try to integrate different security modelsd	LOW	FZU, Hanlin Cai	Fri 10-Mar-23	Fri 31-Mar-23	16		10%
4	Comprehensive experiments	NORMAL	FZU, Hanlin Cai	Sat 01-Apr-23	Mon 24-Apr-23	23		2%
4.1	Collect the data	NORMAL	FZU, Hanlin Cai	Sat 01-Apr-23	Thu 20-Apr-23	14		5%
4.2	Contrast various results	NORMAL	FZU, Hanlin Cai	Wed 12-Apr-23	Mon 24-Apr-23	9		2%
4.3	Analyze and comment on the experiments	HIGH	FZU, Hanlin Cai	Mon 24-Apr-23	Mon 24-Apr-23	0		0%
5	Report writing and revise (Repeatedly)	HIGH	Hanlin Cai	Thu 04-May-23	Wed 24-May-23	21		0%
6	Final demo slides perpared for the research defence	NORMAL	Hanlin Cai	Sat 20-May-23	Sun 28-May-23	9		0%
7	Final research report revision and submission	HIGH	Hanlin Cai	Tue 30-May-23	Mon 12-Jun-23	14		0%

	Question	Objective
RQ1	What are the common security vulnerabilities of current IoT systems and the principles of specific security attacks, such as spoofing, denial of service (DoS) and intrusion attacks?	To understand different security requirements, challenges, and need to secure IoT systems from hostile and massive attacks.
RQ2	What is machine learning based security scheme and the state-of-the-art algorithms for preventing specific IoT attacks, such as spoofing attacks and DoS attacks?	To identify vastly adopted and dependable ML-based methods by existing research to protect IoT systems from specific attacks.
RQ3	What is multiple IoT attacks and how can we combine the advantages of various ML-based security methods to defend against multiple IoT attacks?	To analyze the complicated security attacks in the real-operating environment of the IoT systems and integrate the most advanced defense schemes to improve the security.

Summary: In a word, this week I take most of my time to write the IP Proposal and read related research paper. An in-deep literature review has been conducted to analyse and compare the strength and weakness of existing works. Based on the review, I organize the research workflow and develop an experimental schedule. Finally, a research questions table is presented to illustrate the main challenge and objective in my future research. Again, my IP proposal can be accessed here: https://caihanlin.com/mypaper/IP/Proposal.pdf