A RISK-BASED OPTIMIZATION MODEL FOR ELECTRIC VEHICLE INFRASTRUCTURE RESPONSE TO CYBER ATTACKS

PROJECT THESIS

Submitted in partial fulfillment of the requirements

for the award of degree of

BACHELOR OF TECHNOLOGY AND MASTER OF TECHNOLOGY

in

ELECTRICAL ENGINEERING

By

Gunna Srinivas
(EE14B087)

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY MADRAS, CHENNAI

MAY-2019

THESIS CERTIFICATE

This is to certify that the project work entitled "**A Risk-Based Optimization Model For Electric Vehicle Infrastructure Response To Cyber Attacks"** submitted by **Gunna Srinivas ,** EE14B087, to **Indian Institute of Technology Madras** in partial fulfillment of the requirements for the award of degree of **Bachelor of Technology** and **Master of Technology**, is a bona-fide record of work carried out by him. The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Dr. K Shanti Swarup

Professor, Project Guide

Dept. of Electrical Engineering

IIT-Madras, 600036

Place: Chennai

Date:

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude towards several people who enabled me to reach this far with their timely guidance, support and motivation. First and foremost, I offer my earnest gratitude to my guide, Dr. K Shanti Swarup whose knowledge and dedication has inspired me to work efficiently on the project and I thank him for invaluable comments and suggestions throughout the course of this project. I consider myself fortunate to work with a fun-loving yet sincere group of team- mates. I would like to thank Harsha, Jadhav Pradeep, Vibin, Anvesh, Vasu Bhimani and Murugan Sir for making this journey enjoyable. My deepest gratitude to my mother and father for their tremendous amount of support, encouragement, patience, and prayers.

ABSTRACT

KEY-WORDS

Electric Vehicle, EVCE, Cyber-Attack, Response Model, Smart Grid

As Electric Vehicles are getting connected and intelligent nowadays it opens a lot of opportunities for hackers or attackers. After integration of information and communication technologies in electric vehicle infrastructure attackers can have huge impact on whole smart grid just by compromising one Electric Vehicle or Electric Vehicle charging Equipment. In this analysis Cyber attack is considered to spread in two ways, i.e., through Electric Vehicle charging (Type-1) and the EVCE communication network (Type-2). The ideas based on isolation does not work well in smart grid as most the equipments that depend on electricity always has a constraint on availability.

So a probabilistic cyber-attack propagation model is formulated to estimate the threat levels of EVCEs and an optimized model in response of cyber-attack is proposed. This optimization model helps in finding the optimal combination of removing a set of compromised EVCEs and that are probably going to be compromised from the electric vehicle infrastructure. As a result the risk of cyber-attack propagation minimizes while providing a required amount of equipment to supply demand.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

NOMENCLATURE

Θ : Set of detected compromised EVCEs

M : Number of detected compromised EVCEs

x_j : Binary decision variable which equals to 1 if EVCE $_j$ is kept connected to the network, and 0 otherwise

$U_j(t)$: Random variable which equals to 1 if EVCE $_j$ is compromised at time t, and 0 otherwise

$U_{ij}(t)$: Random variable which equals to 1 if EVCE $_j$ is compromised by EVCE $_i$ at time t, and 0 otherwise

V_j : Random variable which equals to 1 if a cyber attack propagates to and compromises EVCE $_j$, and 0 otherwise

V_{ijk} : Random variable which equals to 1 if a cyber attack propagated from EVCE $_i$ and targeting EVCE $_j$ compromises the k th communication relay between EVCE $_i$ and EVCE $_j$, and 0 otherwise

$\vartheta_j(t)$: The probability of an EVCE being compromised

L_i : Number of EVs charge at EVCE $_i$

L_{ij} : Number of EVs charge at EVCE $_i$ and move to EVCE $_j$ for recharging

β : The probability that an attack propagates without being detected

η : The probability that an attack propagates through a communication relay

γ : The probability that an attack compromises the EVCE at destination

D_{ij} : Hop distance between EVCE $_i$ and EVCE $_j$ in the communication network

Δt : Time duration that a propagation attempt takes

C_j : Number of EVs that can be charged simultaneously at EVCE $_j$

ρ : Unsatisfied demand threshold

ψ : Maximum acceptable risk of demand exceeding the threshold

W : Maximum threat level of the connected EVCEs

CHAPTER 1

INTRODUCTION

1.1 Project Motivation

Security of the smart grid is in danger when the weaknesses of the electric vehicle (EV) infrastructure is not presented properly. The integration of transportation and power systems may leave many open ways to attackers particularly in the interconnected condition, i.e., the electric vehicle infrastructure which includes EVs, EVCEs. In fact, a cyber attack can be propelled from any part of the power or electric systems. If the attack is programmed to be propagated for example a malware or a worm, it can spread further and contaminate different segments, utility computers and servers of the operator [1].

There are in excess of 17,000 electric power substations in the U.S. and Canada. Each contains various electric power equipments which includes electrical relays, power transformers, phase-shifting transformers and capacitor banks. Various automation and communication equipment are used to measure, monitor, and control these power grid components [2].

The latest Risk Management Process rule created by the Department of Energy, the National Institute of Standards and Technology and the North American Electric Reliability Corporation tells that traditional protection schemes are not that useful in the energy sector [3].

With the integration of data and Communication Technologies attacks have turned out to be progressively penetrable. Nowadays hackers can enter any section or unit of the cyber-physical energy infrastructure and recruit agents which directs the electrical grid to an insecure state. With the increase of usage in EVs which makes transportation to depend on the availability of the power grid. A blackout in the power grid will cripple the electric transportation which is a genuine worry for electric public safety vehicles as they also depend on the power grid. This interdependency makes the smart grid highly appealing for attackers or hackers.

1.2 Objectives

The main objectives of this project are as follows

1. To develop a model that mimics cyber attacks
2. Build up a response model that limits the danger of cyber-attack propagation while at the same time giving a adequate level of equipment available to supply demand.

1.3 Scope

In this project we considered EVCE demand is uniformly distributed but the demand might not be uniformly distributed it might show variations and one kind of distribution cannot represent all cases.

The risk parameter ψ is a predetermined input to the cyber attack response model in this project but it can be integrated as a tunable parameter to the cyber attack response model.

1.4 Thesis Structure

Chapter 2 briefs about Electric vehicle charging equipment and why we need information and communication technologies in Electric vehicle infrastructure.

Chapter 3 is about estimating the threat levels of the EVCEs (Electric Vehicle cahrging Equipments) when one or more EVCEs are detected as compromised by formulating the attack propagation model.

Chapter 4 is about formulating response model as a MILP - Mixed Integer Linear programming model that determines which EVCEs should be removed from the service such that maximum threat level is minimized while demand is within a certain threshold.

Chapter 5 is about modeling the 5-EVCE test system and 20-EVCE test system with randomly generated data and try to find the correct combination of EVCEs that should be removed from the network.

Chapter 6 gives suggestion for future work and conclusion for this project.

Appendix summarizes the python code that is used to get the results.

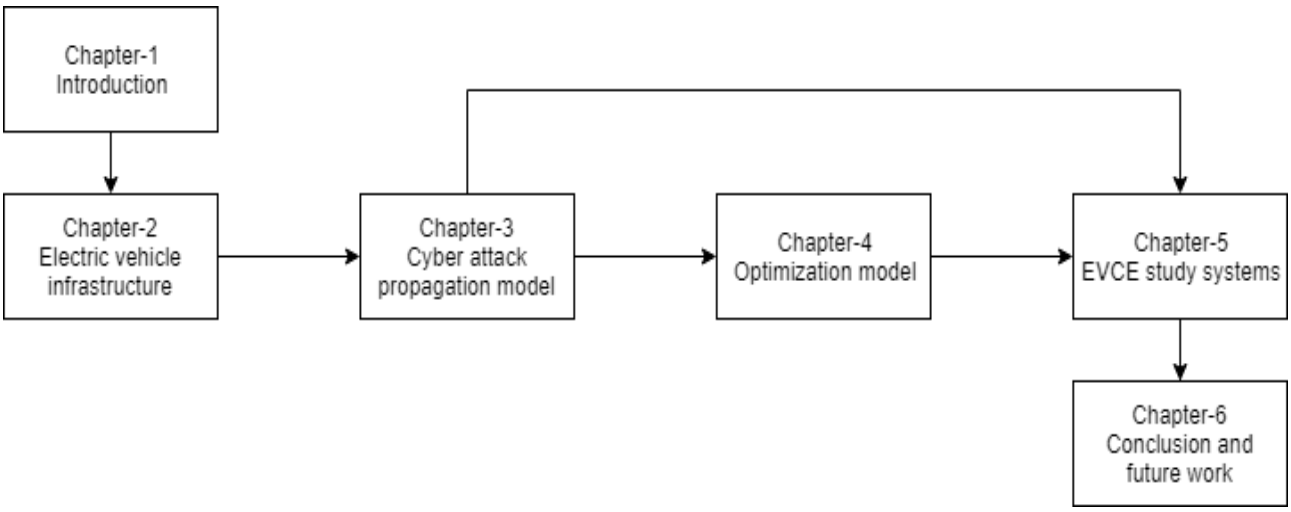

fig 1.1 Flow chart of thesis structure

CHAPTER 2

ELECTRIC VEHICLE INFRASTRUCTURE

2.1 Introduction

Electric Vehicle Infrastructure is nothing but the combination of Electric Vehicles, Electric Vehicle charging Units (EVCE's) and Communication network. The EVCEs are connected to control center or base station and they are also connected to charging service provider through wireless front end that is connected to routers at the backhaul.

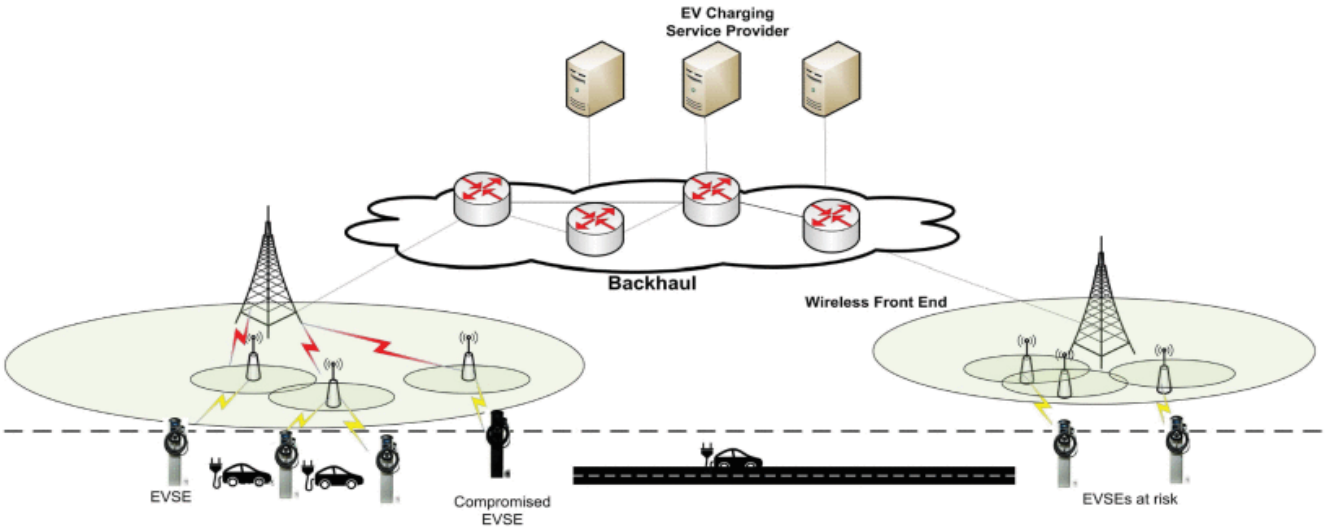

Fig 2.1. Overview of system architecture [4]

2.2 Electric Vehicle Charging Equipment (EVCE)

Electric vehicle charging equipment is commonly known as charging station or charging dock. Charging stations are built for the electrical safety of the user, the vehicle and the power grid.

A charging station(Level 1 (120V) station or a Level 2 (240V) station) will provide AC power to the vehicle for charging which is converted to DC power and used to recharge the batteries. The actual charger is on-board the vehicle. A charging station uses several layers of redundant safety features to protect the user from electrical hazards while connecting and disconnecting the station to the vehicle.

Once connected to the vehicle, the station informs the vehicle that power is available and at what level. From that point, the vehicle takes over, initiates and takes full control of the power transfer.

fig 2.2. Electric vehicle charging equipment [5]

2.3 Requirement of Information and Communication Technologies in Electric vehicle Infrastructure

The varying temporal and spatial demand patterns of Electric Vehicles threatens power grid operations and its physical components. Thus, the ability of the power grid to handle the potential extra load has become a major factor in the mainstream success. For this to happen the consumers and power grid should be coordinated

Controlling EV charging can reduce the number of overload network components which need to be replaced which eliminate the need for costly upgrades. It is further shown that controlling EV charging can reduce the cost of energy losses by 20% when compared to uncontrolled charging. To control charging we need communication between electric vehicles and EVCEs.

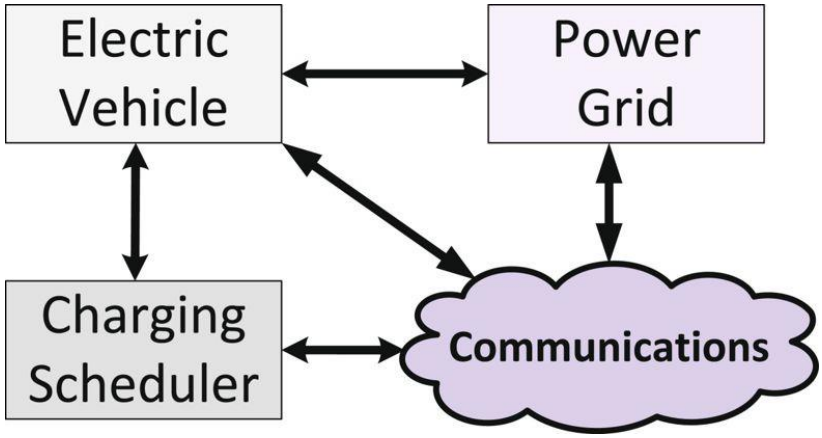

fig 2.3. Interdependency of communications and EV demand management [6]

Mobile EVs use public fast charging stations to fill up their batteries. We know that customer demand varies both spatially and temporally (example - high demand during rush hours). Also, the current status of the power grid limits grid operators to deploy the required number of charging stations. Hence, customer demand should be balanced among neighboring stations through the use of communication infrastructures. Thus, the ability to share data for mobile EVs becomes a necessity. In figure 2.4 , we present an overview of message exchange in electric vehicle networks.

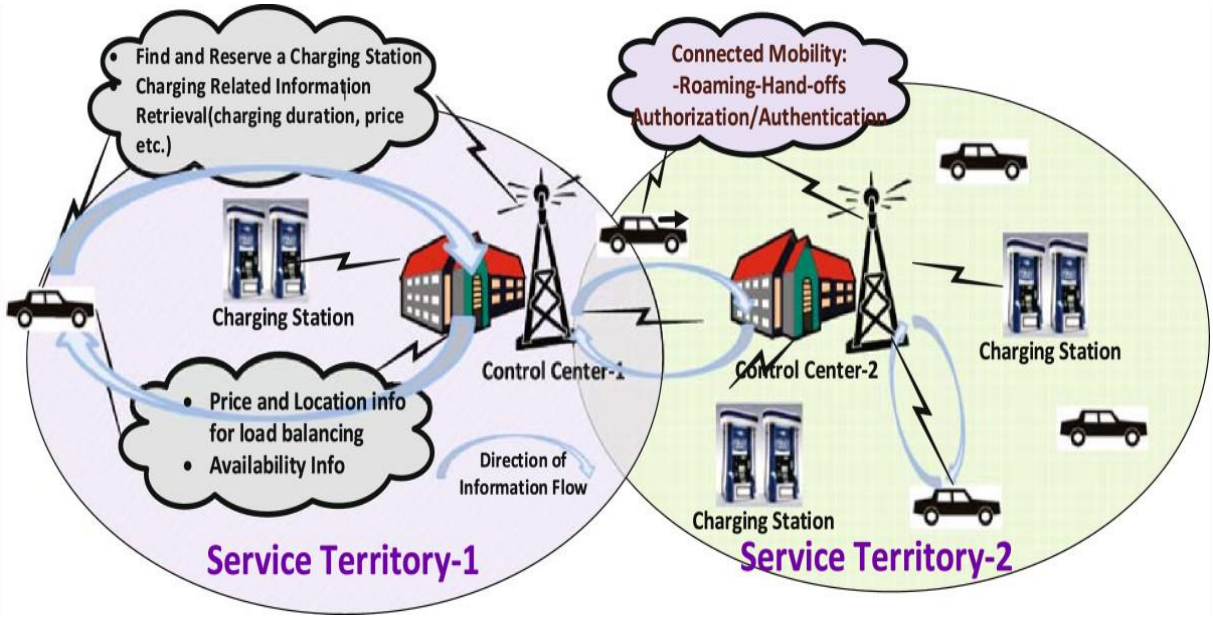

fig 2.4. Overview of message exchange in electric vehicle networks [7]

If there is no communication between EV and EVCE many people might go to same location and overloading it by neglecting the other EVCE near to that which means inefficient use of resources

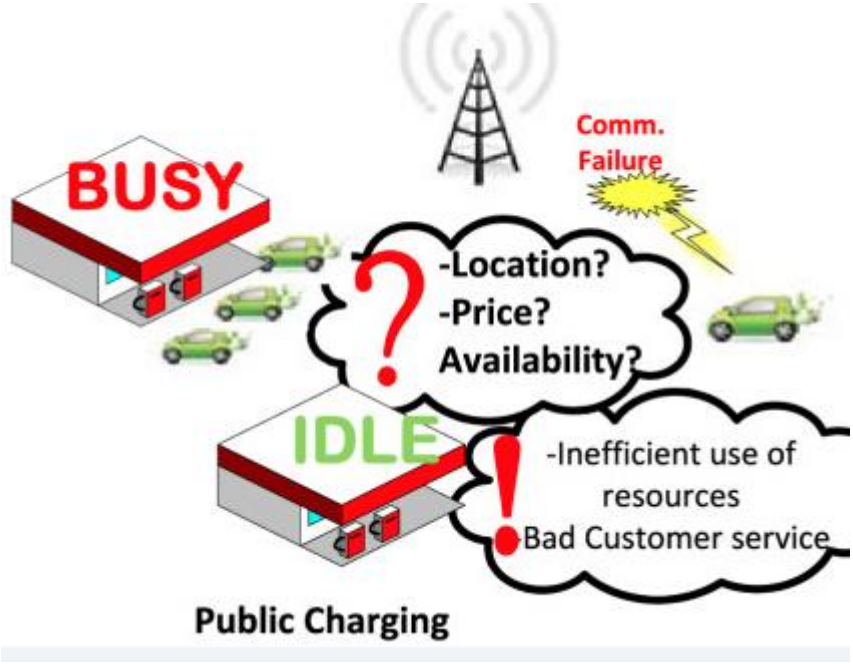

fig 2.5. Negative effects of communication unavailability [8]

2.4 Summary

This chapter gives a basic introduction of Electric Vehicle charging Equipment (EVCE) and why we need information and communication technologies in Electric Vehicle Infrastructure is discussed.

CHAPTER 3

CYBER-ATTACK PROPAGATION MODEL

3.1 Introduction

In this project the cyber attack is considered to spread in two ways, i.e., through Electric Vehicle charging (Type-1) and the EVCE communication network (Type-2). A probabilistic equation is formulated to find the threat levels of EVCEs at time t.

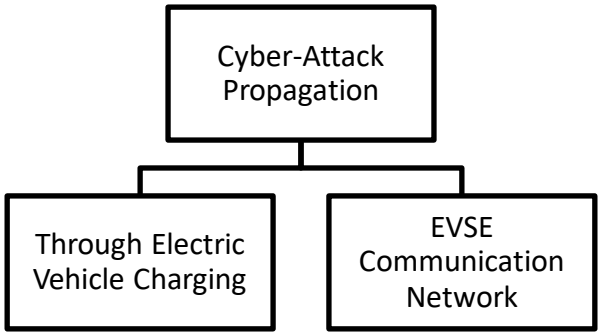

fig 3.1. Ways of cyber-attack propagation

3.2 Cyber - Attack Propagation In The Network

Cyber attack is considered to spread in two ways in this analysis, i.e., through Electric Vehicle charging (Type-1) and the EVCE communication network (Type-2).

Some examples of Type-1 are: malware downloaded as a software fix from an source which is not trusted, or a traded off mobile application that communicates with the Electric Vehicle and downloads a malware. Type-II attacks start either from Electric Vehicles or EVCEs, and they propagate from one EVCE to the next. An example situation of Type-2 comes from a network of charging stations that share usage information with one another to improve administrator's service.

3.3. Formulating The Cyber - Attack Propagation Model

3.3.1. Initial Threat Level Of EVCEs

M EVCEs are compromised at time t = 0. At time t = 0 the other EVCEs might also get compromised but these EVCEs can be compromised only by charging Electric Vehicles that are already charged from a compromised EVCE. Cyber attack propagation through communication network is not considered at t = 0 because for the attack to propagate between to 2 EVCEs it requires some time t. Following is the formulation for threat level at t = 0.

$$\theta j(0) = 1 \qquad \forall\, j \in \Theta \tag{3.1}$$

$$\theta j(0) = \Pr(Uj(0) = 1)$$

$$\theta j(0) = 1 - \Pr(Uj(0) = 0)$$

$$\theta j(0) = 1 - \prod_{i\epsilon\Theta, i\neq j}(1 - \Pr(Uij(0) = 1))$$

$$\theta j(0) = 1 - \prod_{i\epsilon\Theta, i\neq j}(1 - \beta\,(\tfrac{\mathrm{Lij}}{\mathrm{Li}}))\ \ \forall\, j \notin \Theta \tag{3.2}$$

3.3.2. General Threat Level Formula

After finding the compromised EVCEs they are removed from the electric vehicle infrastructure but even after removing the attack continues to propagate via communication network. Let t denote the time that a propagation attempt takes in the communication network and K Δ t denote the inspection period [8]. Equation (3.3) holds to estimate the threat levels of EVCEs at time t = t

$$\begin{aligned}\theta j(\Delta t) &= \Pr(Uj(\Delta t) = 1)\\ \theta j(\Delta t) &= \Pr\{(Uj(\Delta t) = 1 | Uj(0) = 0)\\ &\quad * \Pr(Uj(0) = 0)\\ &\quad + \Pr\{(Uj(\Delta \mathrm{t}) = 1 | Uj(0) = 1)\}\\ &\quad * \Pr(Uj(0) = 1) \qquad \forall j \notin \Theta\end{aligned} \tag{3.3}$$

The second term in equation (3.3), Pr($U_j(0) = 0$) is equivalent to $1-\theta_j(0)$, the third term, Pr{$U_j(\Delta t) = 1 | U_j(0) = 1$)} is equivalent to 1 and the fourth term, Pr($U_j(0) = 1$) is equivalent to $\theta_j(0)$. The first term from equation (3.3), A = Pr{$U_j(\Delta t) = 1 | U_j(0) = 0$)}, is determined below.

$$A = 1 - \Pr\{Uj(\Delta t = 0 | Uj(0) = 0\}$$
$$A = 1 - \prod_{\substack{i \notin \Theta \\ i \neq j}} (\Pr\{Uj(\Delta t) = 0 | Ui(0) = 1)\})$$
$$A = 1 - \prod_{\substack{i \notin \Theta \\ i \neq j}} (1 - \alpha ij * \theta i(0)) \qquad (3.4)$$

where α_{ij} is the probability that the attack propagates from compromised EVCE $_i$ to an uncompromised EVCE $_j$ during the time period of t as given by equation (3.5).

$$\alpha ij = \Pr(Vj = 1) * \prod_{k=1}^{Dij} \Pr\{Vijk = 1\}$$
$$\alpha ij = \prod_{k=1}^{Dij} \eta$$
$$\alpha ij = \gamma \eta^{Dij} \qquad i, j \notin \Theta \qquad (3.5)$$

By replacing equation (3.4)-(3.5) in equation (3.3), we obtain the threat level of *EVCE* $_j$ at time $t = t$, $\theta_j(t)$, given in equation (3.6)

$$\theta j(\Delta t) = 1 - \big(1 - \theta j(0)\big) \prod\nolimits_{i \notin \Theta, i \neq j} \big(1 - \alpha ij * \theta i(0)\big) \quad \forall j \notin \Theta \qquad (3.6)$$

The general threat level formula is given in equation (3.7).

$$\theta j(0) = 1 - \prod_{\substack{i \in \Theta \\ i \neq j}} (1 - \beta * \left(\frac{Lij}{Li}\right))$$

$$\theta j(n\Delta t) = 1 - \Big(1 - \theta j\big((n-1)\Delta t\big)\Big) * \Big(\prod_{\substack{i \notin \Theta \\ i \neq j}} (1 - \theta i\big((n-1)\Delta t\big) * \alpha ij)\Big) \quad \forall j \neq \Theta; 1 \leq n \leq K \tag{3.7}$$

3.4 Summary

This chapter discuss about the step by step formulation of attack propagation model and also the ways of attack propagation in electric vehicle infrastructure.

CHAPTER 4

RISK-BASED OPTIMIZATION MODEL IN RESPONSE OF CYBER-ATTACK

4.1. Introduction

At the point when a cyber-attack happens in the EVCEs network, the typical practice is to remove the recognized compromised EVCEs from service. In this project, we suggest that the compromised EVCEs and those which are probably going to be compromised will be removed from service as long as the required capacity demand of the Electric Vehicles is met. Our methodology plans to hinder the propagation pace even further until the network is completely assessed and recovered.

The proposed response approach is formulated as a MILP model that figures out which EVCEs ought to be removed from service such that the maximum threat level of the EVCEs connected to the network by the time of inspection is minimized while the risk of lack of supply is within a certain threshold.

4.2. Objective Function Formulation

The risk (threat) levels determined by equation (3.7), should be altered to consider removal of the probably compromised EVCEs at the end of examination. After examination, these EVCEs are no longer connected to the network and cannot spread the attack. The remaining connected EVCEs keep on spreading the attack until the network is completely recovered by installing trusted patches from reliable sources. xj a binary decision variable is used to address the status of connection of the EVCEs in the threat levels formulation which can be seen in equation (4.1)

$$\theta j(0) = 1 - \prod_{\substack{i \in \Theta \\ i \neq j}} (1 - \beta * \left(\frac{Lij}{Li}\right))$$

$$\theta j(n\Delta t) = 1 - \Big(1 - \theta j\big((n-1)\Delta t\big)\Big) * \Big(\prod_{\substack{i \notin \Theta \\ i \neq j}} (1 - \theta i\big((n-1)\Delta t\big) * \alpha ij * xj)\Big) \quad \forall j \neq \Theta; 1 \leq n \leq K \tag{4.1}$$

Equation (4.1) is nonlinear for n ≥ 1. Equation (4.1) is rearranged and log is applied on both sides so that the equation becomes linear and is given in equation(4.3)

$$ln(1-\theta j(n\Delta t) = \sum_{\substack{i\notin\Theta \\ i\neq j}} ln\big(1-\theta i\big((n-1)\Delta t\big)*\alpha ij*xj\big) + ln\Big(1-\theta j\big((n-1)\Delta t\big)\Big) \qquad (4.2)$$

The above equation can be written is equivalent linear fashion as follows

$$\ln(1-\theta j(n\Delta t) = \sum_{\substack{i\notin\Theta \\ i\neq j}} xi*\ln\big(1-\theta i\big((n-1)\Delta t\big)*\alpha ij\big) + \ln\Big(1-\theta j\big((n-1)\Delta t\big)\Big) \qquad (4.3)$$

The objective function is to minimize the maximum threat level of all connected EVCEs by the time of inspection and is given as follows

$$Z = \min\max(\,\theta j(K\Delta t)*xj) \quad \forall j \notin \Theta \qquad (4.4)$$

As the objective function given above is Non Linear the Linear version of objective function is given as follows

$$Z = \min\max(-ln(1-\theta j(K\Delta t))*xj) \quad \forall j \notin \Theta \qquad (4.5)$$

4.3. Constraints For Objective Function

Let $yj = -\ln(1-\theta j(K\Delta t) * xj$ and $W = \max j(yj)$. We can now write the objective function as in equation (4.6). But we need constraints, as given in equations (4.7)-(4.11), to represent these new definitions in a linear fashion

$$Z = \min W \tag{4.6}$$

Subject to:

$$yj \leq xj \quad \forall j \notin \Theta \tag{4.7}$$

$$yj \leq -ln\big(1-\theta j(K\Delta t)\big) \quad \forall j \notin \Theta \tag{4.8}$$

$$yj \leq -ln\big(1-\theta j(K\Delta t)\big) - (1-xj) \quad \forall j \notin \Theta \tag{4.9}$$

$$yj \geq 0 \quad \forall j \notin \Theta \tag{4.10}$$

$$yj \leq W \quad \forall j \notin \Theta \tag{4.11}$$

Following equation is utilized to keep the EVCEs with threat levels lower than a threshold value of T_j connected to the network

$$\theta j(K\Delta t) > Tj - xj \quad \forall j \notin \Theta \tag{4.12}$$

The linear version of equation (4.12) is given in equation (4.16)

$$1-\theta j(K\Delta t) < 1 - Yj + xj \tag{4.13}$$

$$\ln\big(1-\theta j(K\Delta t)\big) < \ln(1-Tj+xj) \tag{4.14}$$

$$\ln\big(1-\theta j(K\Delta t)\big) < (1-xj) * \ln(1-Tj) + xj * ln(2-Tj) \tag{4.15}$$

$$\sum_{\substack{i\notin \mathrm{j} \\ \mathrm{i}\neq \mathrm{j}}} xi * \ln\big(1-\theta i\big((K-1)\Delta t\big) * \alpha ij\big) + \ln\Big(1-\theta j\big((K-1)\Delta t\big)\Big)$$
$$< (1-xj) * \ln(1-Tj) + xj * \ln(2-Tj) \tag{4.16}$$

Following equation is the constraint to make sure that the risk of unsatisfied demand exceeding a certain threshold value is controlled

$$\Pr(DEV - \sum_{j \in \Upsilon} Cjxj > \rho) \leq \Psi \tag{4.17}$$

Where in equation (4.17) C_j is the number of EVs that can be charged simultaneously at $EVCE_j$ and D EV is the forecasted demand for the Electric Vehicle charging stations during the recovery period

We assume demand is uniformly distributed from 0 to D_{max} . Considering the cumulative uniform distribution function of $F(x) = x / D_{max}$ equation (4.17) can be written as follows

$$\Pr(DEV - \sum_{j \in \Upsilon} Cjxj > \rho) = \Pr(DEV > \rho + \sum_{j \in \Upsilon} Cjxj)$$

$$\Pr(DEV - \sum_{j \in \Upsilon} Cjxj > \rho) = 1 - \Pr(DEV \leq \rho + \sum_{j \in \Upsilon} Cjxj)$$

$$\Pr(DEV - \sum_{j \in \Upsilon} Cjxj > \rho) = 1 - (1/\mathrm{Dmax})(\rho + \sum_{j \in \Upsilon} Cjxj) \leq \Psi \tag{4.18}$$

Supply risk constraint can be written as follows

$$\sum_{j \notin \Theta} Cjxj \geq Dmax(1 - \Psi) - \rho \tag{4.19}$$

4.4 Summary

This chapter discuss about the objective function formulation and also the constraints of the objective function.

CHAPTER 5

EVCE STUDY SYSTEM

5.1. EVCE Study System - I Five EVCE

5.1.1 Introduction

5 EVCEs are placed at 5 different location namely CS1, CS2, CS3, CS4, CS5 where CS means charging station. The randomly generated data of proportion of EVs moving between EVCEs are given in Table 5.1 which effects the threat level of EVCEs at time t=0. Randomly generated hop distances are given in Table 5.2. Hop distance is nothing but the count of communication relays between EVCEs and if the hop distance is high it makes difficult for cyber-attack to propagate.

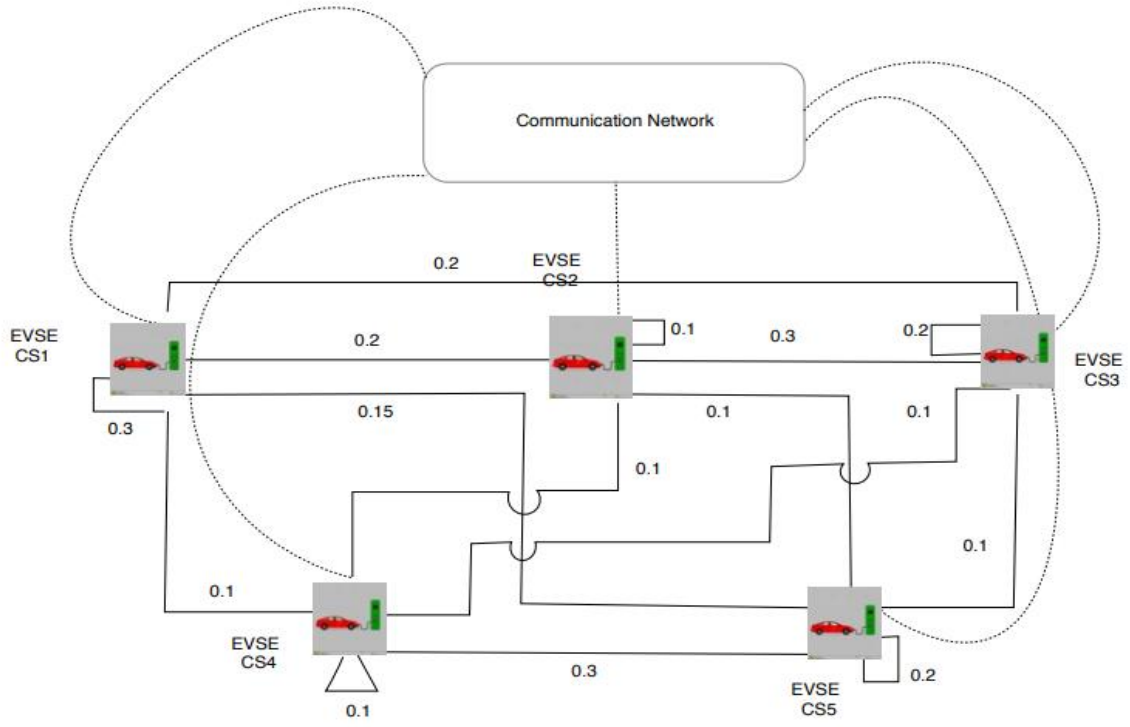

fig 5.1. 5-EVCE system diagram

5.1.2. Input Data For Analyzing The Five-EVCE System

The data used for used for analysis in this project is given in this section, η = 0.05, γ = 0.05. We set t = 0.5 (s), β = 0.1 and T_j = 0.05 (Threshold value for threat level). The inspection time is set to 2 minutes. An assumption is made that demand is uniformly distributed between 0 and 10, D_{max} = 10. Also, the risk of demand exceeding the available capacity by two units is set to be less than 10%, i.e., ρ = 2, ψ = 10%. By substituting ρ, ψ and D max in equation (4.19) tells that the available charging capacity should be equal or greater than seven.

Table 5.1 - Proposition of EV movement between EVCEs (5-EVCE)

EVCE	CS1	CS2	CS3	CS4	CS5	Others
CS1	0.3	0.2	0.2	0.1	0.15	0.05
CS2	0.2	0.1	0.3	0.1	0.1	0.2
CS3	0.2	0.3	0.2	0.1	0.1	0.1
CS4	0.1	0.1	0.1	0.1	0.3	0.3
CS5	0.15	0.1	0.1	0.3	0.2	0.15
Others	0.05	0.2	0.1	0.3	0.15	0.2

Following table is the data for Hop Distances In The EVCE Network

Table 5.2 - Hop distances in the EVCE network (5-EVCE)

EVCE	CS1	CS2	CS3	CS4	CS5
CS1	-	1	2	1	3
CS2	1	-	2	3	1
CS3	2	2	-	1	1
CS4	1	3	1	-	1
CS5	3	1	1	1	-

Following table is the data of EVCE capacity

Table 5.3 - EVCE capacity (5-EVCE)

EVCE	Capacity
CS1	Not needed as it is compromised at t = 0

CS2	7
CS3	Not needed as it is compromised at t = 0
CS4	1
CS5	3

5.1.3. Analysis of Five - EVCE System

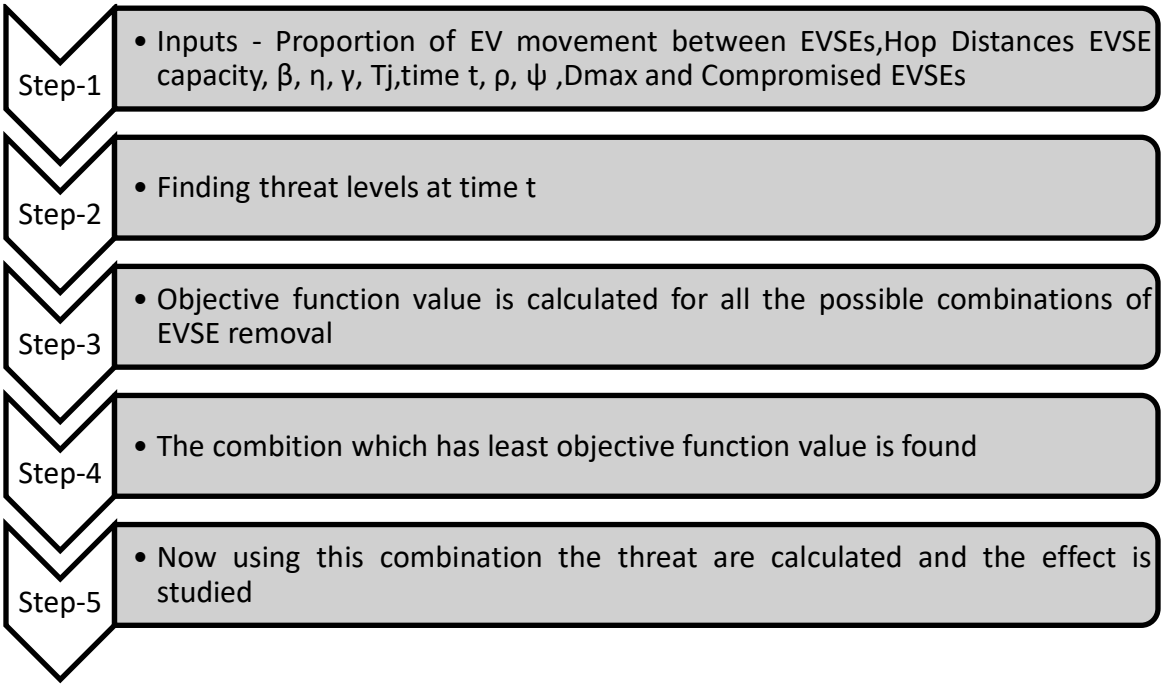

fig 5.2. Flow chart of optimization analysis

In this analysis, we consider that EVCEs CS1 and CS3 are identified as compromised at time *t* = 0. We use initial threat level formula and find initial threat values (t = 0) of EVCE CS2, EVCE CS4 and EVCE CS5 and we can see that the starting threat level of EVCE CS2 is higher than other because a higher percentage of Electric Vehicles from compromised EVCEs CS1 and CS3 was recharged at EVCE CS2.

$$\theta cs2(0) = 0.04940$$

$$\theta cs4(0) = 0.01990$$

$$\theta cs5(0) = 0.02485$$

At the time of detection, the recognized compromised EVCEs are detached from the network. Nonetheless, the remaining EVCEs are probably going to be compromised, with probabilities given above.

Fig. 5.3 demonstrates the threat levels of EVCEs CS2, CS4 and CS5 over time if no action is taken. From figure we can see that the threat levels are increasing nonlinearly. From fig 5.2 notice that EVCE CS5 goes to 1 at a quicker pace even though it threat value at time t = 0 is not the highest. The reason for the quicker pace is the its hop distance between the other two compromised EVCEs is shorter.

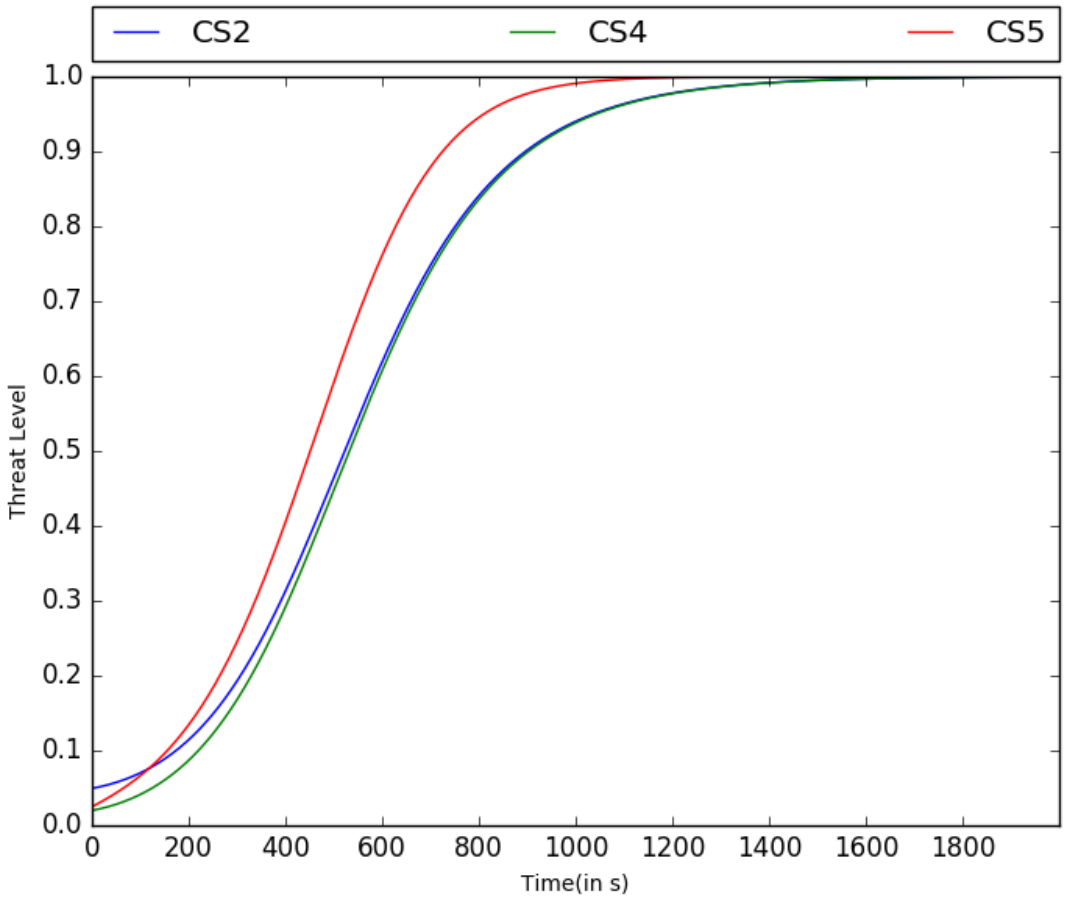

fig 5.3. Threat levels when no action is taken

Fig. 5.4 shows the effect of β on threat levels. For representation we consider the threat levels of EVCE CS2. From figure 3 we can say that the initial threat levels increase as β increases which makes the threat levels increase at a quicker pace since the initial threat levels are higher. A similar pattern is observed for all other EVCEs.

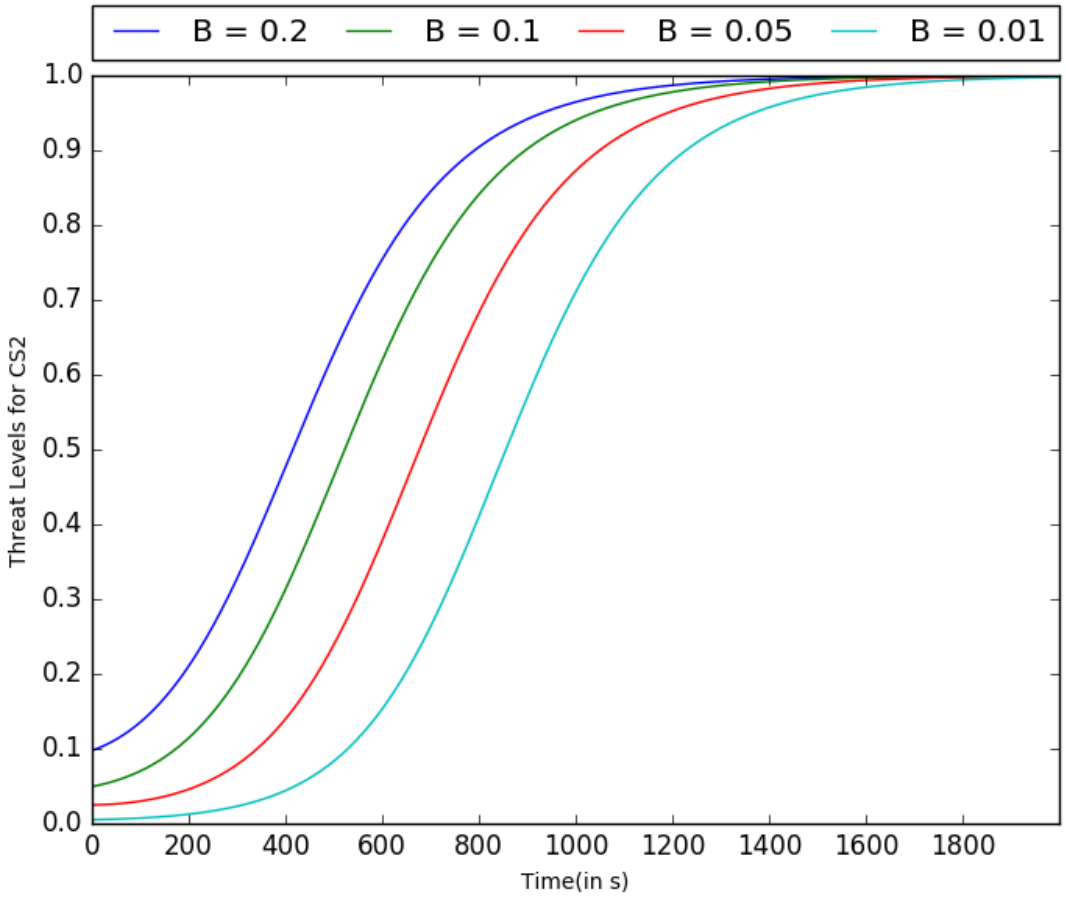

fig. 5.4. Impact of β on threat levels

Fig. 5.5 demonstrates the effect of η on threat levels. We again use the threat level for EVCE CS2 as an instance for demonstration. The threat levels increase at a quicker pace as η increases because the chance of successful propagation from one relay to another increases.

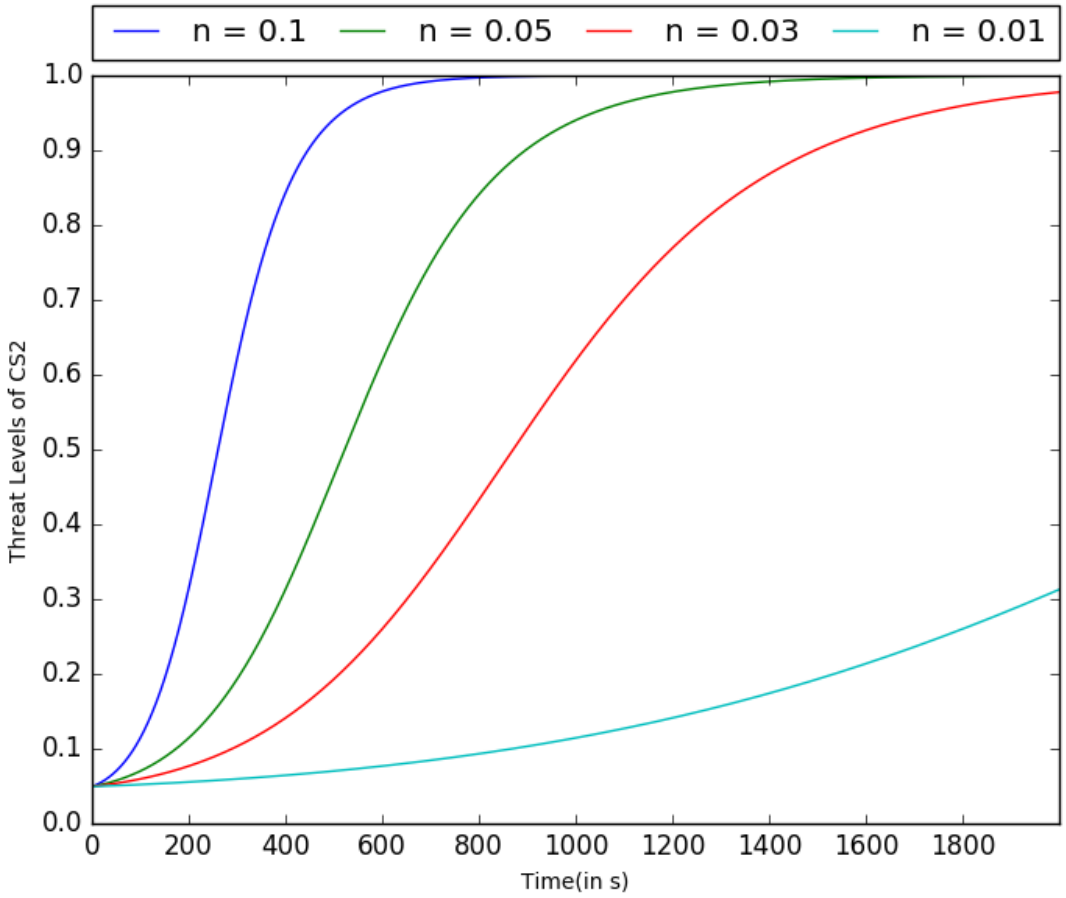

fig. 5.5. Impact of η on threat levels

Since there are 3 likely compromised EVCEs in this situation, there are 8 possible solutions and are given in Table 5.4 yet we overlooked other four solutions as they are infeasible because of the constraint on available capacity. From Table we can conclude that disconnecting EVCE CS1, EVCE CS3 and EVCE CS5 as the optimal solution as it follows all the constraints and have least objective function value.

Table 5.4 - Possible solutions for 5-EVCE system

Disabled EVCEs From Network	Objective Function Value	Available Capacity
CS1, CS3, CS5	0.06079	8
CS1, CS3, CS4, CS5	0.07076	7
CS1, CS3	0.08079	11
CS1, CS3, CS4	0.1052	10

Fig. 5.6 compares the threat levels after implementing the optimal solution and the non-action approach. From fig. 5.6 we can notice that the threat levels are still increasing even after implementing the optimal solution but at a slower pace. Where CS4_NEW are the new threat values estimated by cyber-attack response model.

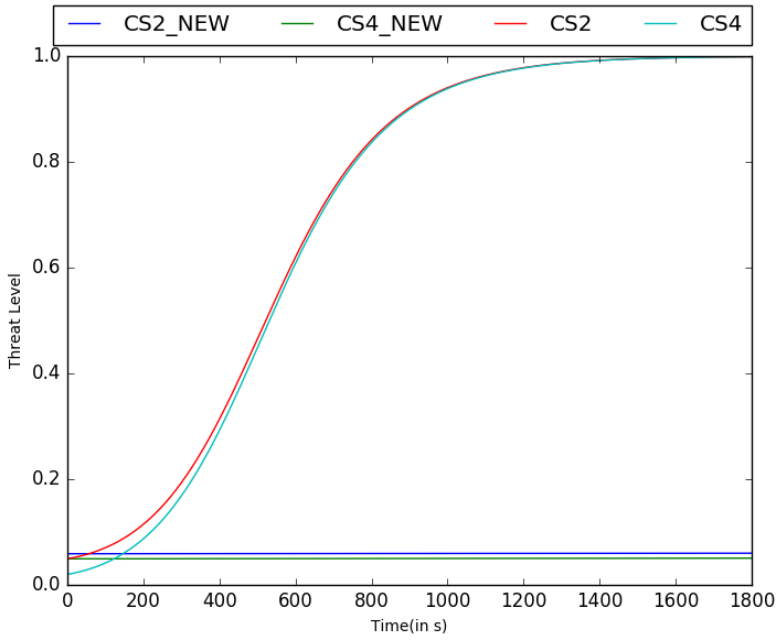

fig. 5.6. Impact of the response model on threat levels

Fig. 5.7 shows the threat values of an EVCE after implementing the optimal solution. We can see the slow pace of increase in threat levels. Here EVCE CS2 is taken as an example.

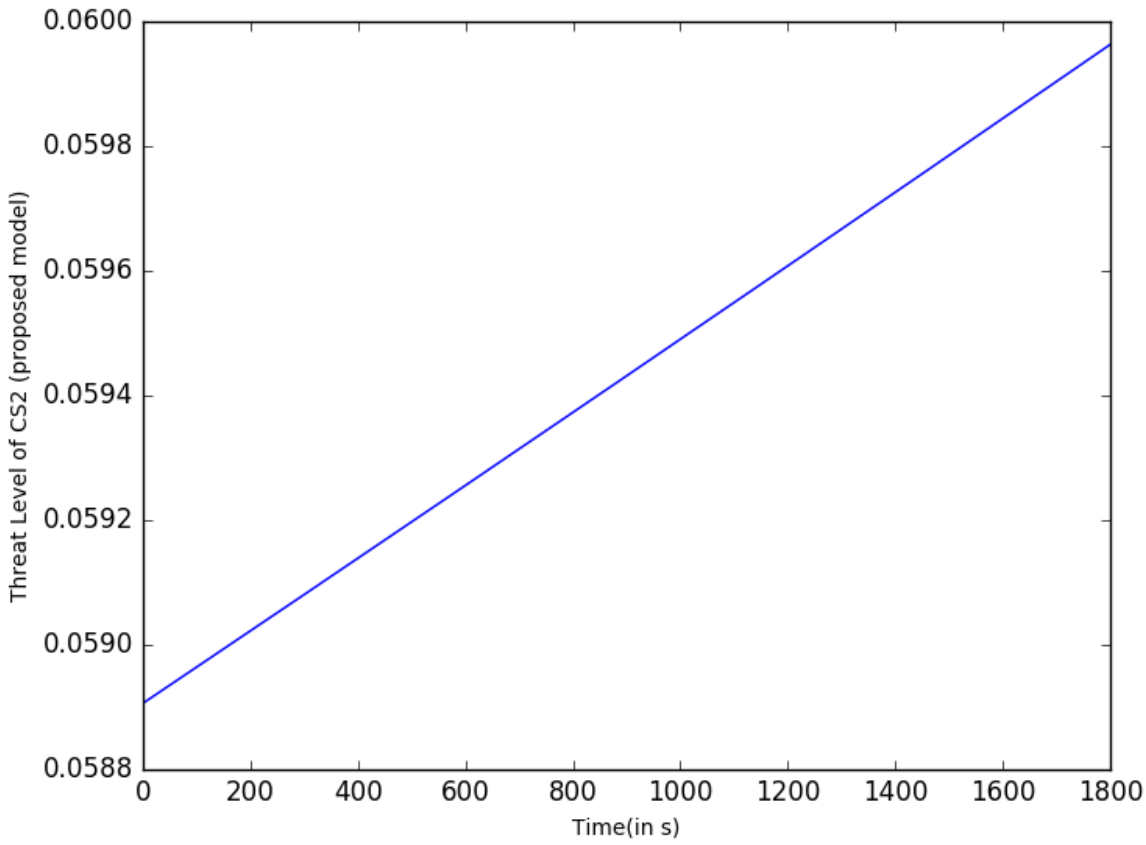

fig. 5.7. Impact of response model on EVCE CS2

5.1.4 Summary

In this chapter we discussed about the input data, analysis of the attack propagation model and optimized cyber-attack response model of 5-EVCE system and also discuss about how the optimized cyber-attack response model effects the 5-EVCE system.

5.2 EVCE Study System - II Twenty EVCE

5.2.1. Introduction

Twenty EVCEs are placed at different locations named as 1, 2, 3....., 20. Analysis is done by using cyber-attack propagation model and optimized cyber-attack response model to find whether the objective function is successful in reducing the pace of propagation of cyber-attack or not. Figure 5.8 shows rough assumption of 20 EVCEs system.

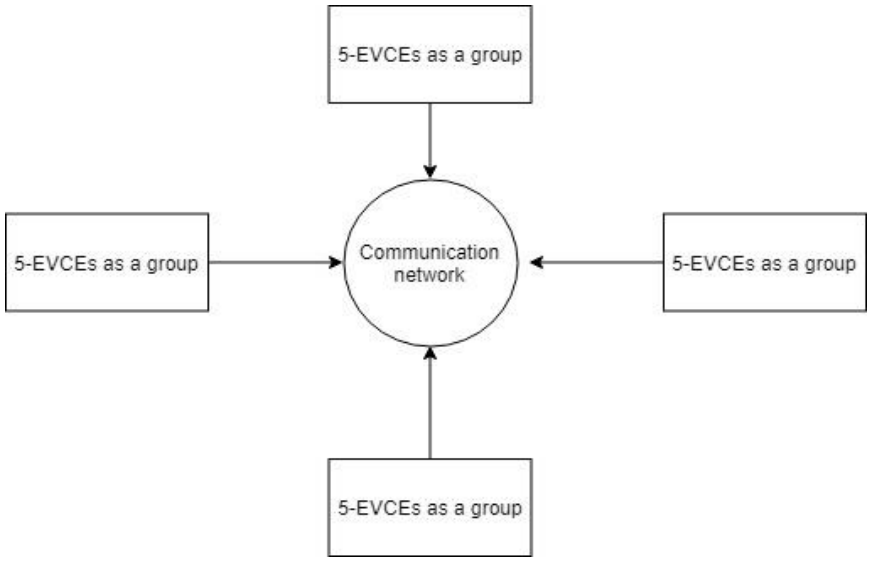

fig 5.8 Equivalent diagram for twenty EVCE system

5.2.2. Input Data For Analyzing Twenty-EVCE system

In table 5.5 the data of proportion of EV movement between EVCEs are given. In table 5.6 hop distances of twenty EVCE system is given where hop distance is nothing but the number of intermediate devices such as routers through which given data must pass between the source and destination. and In table 5.7 charging capacities are given. All values in Table 5.5 are multiplied by 100 to represent them in integral values.

Table 5.5 - Proportion of EV movement between EVCEs (20 - EVCE)

EVCE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	7	3	3	7	4	9	5	3	3	4	9	3	3	5	7	5	7	5	1	7
2	3	5	5	4	2	5	9	2	4	4	2	4	7	2	7	2	9	9	5	9
3	3	5	7	7	4	2	2	4	9	7	6	9	9	2	2	7	3	4	4	4
4	7	4	7	6	2	9	4	8	2	1	6	6	6	4	4	4	9	6	4	1
5	4	2	4	2	8	1	5	4	5	7	5	7	8	7	2	4	5	5	8	7
6	9	5	2	9	1	2	3	8	5	8	5	9	6	6	2	2	8	5	2	3
7	5	9	2	4	5	3	7	4	4	5	6	5	2	6	5	7	2	4	5	10
8	3	2	4	8	4	8	4	5	3	3	6	5	3	3	6	5	8	9	9	2
9	3	4	9	2	5	5	4	3	3	2	3	6	8	6	14	2	8	2	6	5
10	4	4	7	1	7	8	5	3	2	8	2	8	6	2	4	3	7	5	2	12
11	9	2	6	6	5	5	6	6	3	2	6	5	8	5	2	5	8	2	2	7
12	3	4	9	6	7	9	5	5	6	8	5	1	8	5	2	4	8	2	1	2
13	3	7	9	6	8	5	2	3	8	6	8	8	1	2	4	6	7	3	2	1
14	5	2	2	4	7	5	6	3	6	2	5	5	2	2	10	2	3	10	6	12
15	7	7	2	4	2	2	5	6	14	4	2	2	4	10	1	2	3	6	15	2
16	5	2	7	4	4	2	7	5	2	3	5	4	6	2	2	7	1	13	15	4
17	7	9	3	9	5	8	2	8	8	7	8	8	7	3	3	1	1	1	1	1
18	5	9	4	6	5	5	4	9	2	5	2	2	3	10	6	13	1	3	4	2
19	1	5	4	4	8	2	5	9	6	2	2	1	2	6	15	15	1	4	2	6
20	7	9	4	1	7	3	10	2	5	2	7	2	1	12	2	4	1	2	6	3

Table 5.6 - Hop distances (20-EVCE)

EVCE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	-	5	1	4	2	3	3	1	5	3	1	2	5	3	5	1	5	4	4	4
2	5	-	3	4	1	2	4	5	1	5	4	3	2	4	3	3	4	4	5	4
3	1	3	-	5	4	1	5	2	5	3	2	4	5	2	4	5	5	2	3	3
4	4	5	5	-	4	2	4	1	5	2	2	2	1	1	2	3	1	3	5	1
5	2	2	4	4	-	2	4	3	2	4	5	1	1	4	2	5	4	1	4	4
6	3	3	1	2	2	-	5	4	5	4	1	1	3	1	3	5	2	3	2	2
7	3	5	5	4	4	5	-	4	2	2	2	3	1	3	5	3	1	1	5	5
8	1	6	2	1	3	4	4	-	5	4	3	4	5	3	1	3	3	5	1	3
9	5	2	5	5	2	5	2	5	-	4	1	4	3	1	1	5	1	3	1	1
10	3	6	3	2	4	4	2	4	4	-	5	2	2	3	4	4	4	3	4	5
11	1	5	2	2	5	1	2	3	1	5	-	4	1	4	3	1	5	5	5	5
12	2	3	4	2	1	1	3	4	4	2	4	-	1	4	1	5	2	3	1	5
13	5	2	5	1	1	3	1	5	3	2	1	1	-	4	5	2	1	1	2	4
14	3	4	2	1	4	1	3	3	1	3	4	4	4	-	3	1	1	4	5	3
15	5	3	4	2	2	3	5	1	1	4	3	1	5	3	-	3	3	5	5	3
16	1	3	5	3	5	5	3	3	5	4	1	5	2	1	3	-	1	5	4	2
17	5	4	5	1	4	2	1	3	1	4	5	2	1	1	3	1	-	5	4	3
18	4	4	2	3	1	3	1	5	3	3	5	3	1	4	5	5	5	-	4	3
19	4	5	3	5	4	2	5	1	1	4	5	1	2	5	5	4	4	4	-	2
20	4	4	3	1	4	2	5	3	1	5	5	5	4	3	3	2	3	3	2	-

Table 5.7 - EVCEs capacity (20-EVCE)

EVCE	Capacity	EVCE	Capacity
1	2	11	3
2	4	12	1
3	3	13	4
4	2	14	1
5	3	15	3
6	1	16	3
7	3	17	2
8	2	18	4
9	4	19	2
10	1	20	2

5.2.3. Analysis Of Twenty - EVCE System

let EVCEs 1 and 2 are randomly chosen as compromised at time t = 0 and D_{max} is set to 40 and all other values are same as in 5-EVCE test system. Figure 5.9 demonstrates the threat levels of EVCEs if the proposed response model is not implemented. From figure 5.9 we can see that the threat level of EVCE 10 is increasing at a slower pace comparing to other EVCEs because EVCE 10 has the highest average hop distance and EVCE 10 is the only one that does not have a 1-hop distance with the other EVCEs.

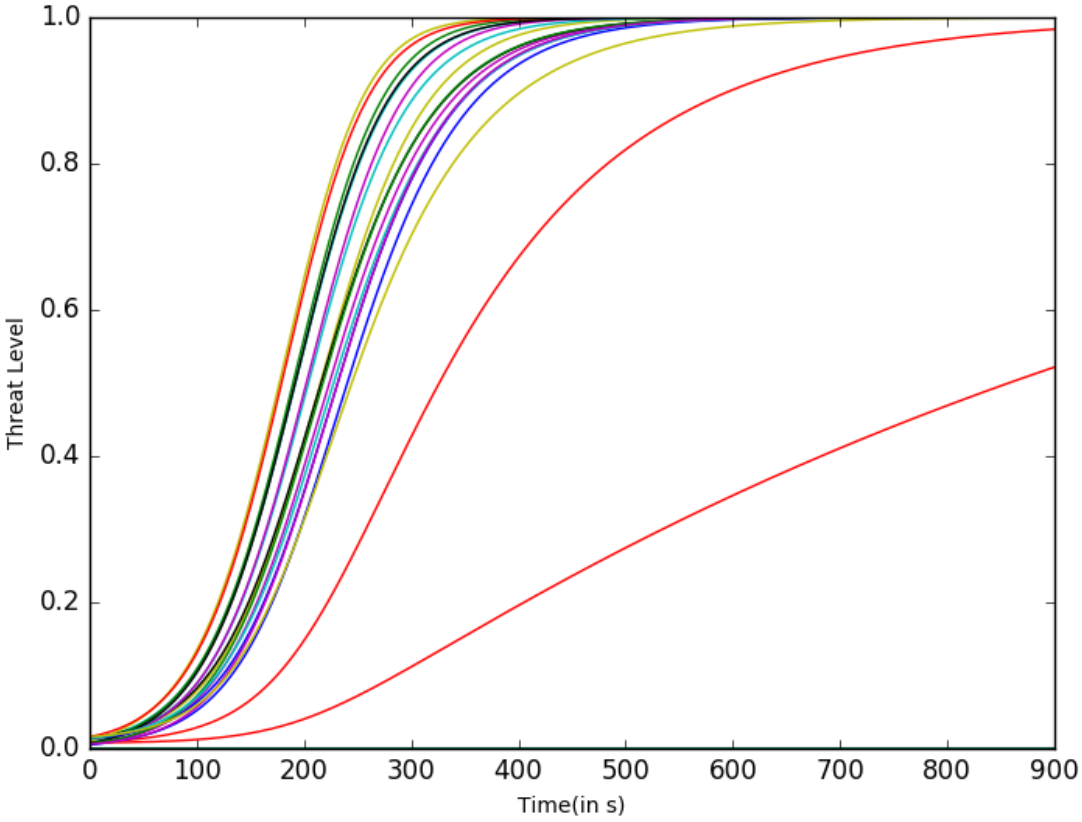

fig. 5.9. Threat levels when no action is taken

We apply proposed response model and some of the solutions are given in the table 5.8 and the top solution in that table is the optimal solution

Table 5.8 - Possible solutions for 20-EVCE system

Disabled EVCEs	Objective Function Value	Available Capacity
1, 2, 4, 11, 12, 17	0.1590	36
1, 2, 9, 12, 13, 14	0.1607	34
1, 2, 6, 9, 13, 14	0.1631	34
1, 2, 12, 13, 14, 17, 20	0.1776	34

Table 5.9 shows the effect of the ψ on optimal solution. From table 5.9 we can notice that as the value of ψ increases the maximum threat level of connected EVCEs decreases.

Table 5.9 - Effect of ψ on Optimal Solution

ψ	Disabled EVCEs	Objective Function Value	Available capacity
0.1	1, 2, 4, 11, 12, 17	0.1590	36
0.15	1, 2, 9, 12, 14, 17	0.1334	36
0.3	1, 2, 4, 6, 9, 12, 13, 17	0.1002	30
0.5	1, 2, 4, 6, 8, 9, 12, 13, 16, 17, 18	0.0656	21

5.2.4 Summary

This chapter discuss about the effect of optimized cyber-attack response model on 20-EVCE system and the effect of risk parameter on the objective function.

CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1. Conclusion

Electrical power systems have turned out to be increasingly defenseless against cyber attacks because of the advancement in data and communication technologies which open up new doors for attackers. Attackers may compromise loads, smart meters, transmission and distribution equipment, PMUs, computers, EVs, EVCEs etc.

In this project, we developed a response model that together minimizes risk and maximizes availability of the smart grid equipment. These attacks can be spread quicker than other different attacks caused because of communication network and vehicle to EVCE communication. In this project, we consider an cyber-attack model where attack can propagate due to both vehicle-to-EVCE and EVCE communications. Utilizing this model, a response model is proposed that averts attacks to spread further into the power grid. This proposed response model is formulated as a MILP problem that minimizes the risk of attack propagation while considering the EV loads, EV threat levels and demand. I can conclude that the response model succeeded in lowering the pace of increasing threat levels which allows us to recover from the attack.

6.2. Future Work

Here we assumed that EVCE demand is uniformly distributed but the EVCE demand might not be uniformly distributed it might show variations and one kind of distribution may not represent all cases. So we can update the model such that the demand follows other distribution functions also.

We have considered the risk parameter ψ as a predetermined input parameter to the proposed response model. In future work we can use the idea of integrating the risk parameter as a tunable parameter to the model.

APPENDIX

PYTHON CODE

A.1. Optimization Code

```
1. import numpy as np
2. from math import log
3. from copy import deepcopy
4.
5. def start_theta(damaged_j, pro):
6.     theta_O = [0.0 for i in range(J)]
7.     for j in range(J):
8.         a1 = 1
9.         for i in range(J):
10.            if i in damaged_j and i!=j:
11.                a1 *= 1 - (0.1*(pro[i][j]))
12.        theta_O[j] = 1-a1
13.    print theta_O
14.    return theta_O
15.
16.def gen_theta(damaged_j, theta_O, alp):
17.    theta_j = [0.0 for i in range(J)]
18.    z1 = [0.0 for i in range(J)]
19.    for i in range(J):
20.        if i not in damaged_j:
21.            theta_j[i] = theta_O[i]
22.    delta_t = 0.5
23.    time = 120
24.    # print damaged_j
25.    K = int(time/delta_t)
26.    for n in range(K+1):
27.        theta_new = [0.0 for i in range(J)]
28.        for j in range(J):
29.            if j not in damaged_j:
30.                a = (1 - theta_j[j])
31.                for i in range(J):
32.                    if i not in damaged_j and i != j:
33.                        a *= (1 - theta_j[i] * (alp[i][j]))
34.                theta_new[j] = 1 - a
35.        if(n == K-1):
36.            z1 = theta_new
37.        theta_j = theta_new
38.    print "theta_j: ", theta_j
39.    return theta_j
40.
41.def gen_combinations(damaged_j, ind, J, alp, init_damaged_j, C_j, D_max, psi,
   rho, ans,pro):
42.    if ind == J:
43.        print "damaged_j: ", damaged_j
44.        # supply risk constraint
```

```
        cx_sum = 0
        a1 = 0
        b1 = 0
        c1 = 0
        for j in range(J):
            if j not in damaged_j:
                cx_sum += C_j[j]
        if cx_sum < (D_max * (1 - psi) - rho):
            return [False]
        theta_0 = start_theta(damaged_j,pro)
        theta_j = gen_theta(damaged_j, theta_0, alp)
        for i1 in range(J):
            a1 = log(1 - z1[i1])
            for j1 in range(J):
                if(j1 not in damaged_j) and (j1 != i1):
                    b1 += log(1 - (z1[j1] * alp[j1][i1]))
            c1 = b1+a1
            if (i1 not in damaged_j) and (c1 >= log(2-0.05)):
                return[False]
        W = -1.0
        for j in range(J):
            if j not in init_damaged_j:
                x_j = 0
                y_j = 0.0
                if j not in damaged_j:
                    x_j = 1
                    y_j = -log(1 - theta_j[j])
                W = max(W,y_j)
                # constraints
                if (y_j > x_j):
                    return [False]
                if (y_j > -log(1 - theta_j[j])):
                    return [False]
                if (y_j < (-log(1 - theta_j[j]) - (1 - x_j))):
                    return [False]
                if (y_j < 0):
                    return [False]
        ans.append([deepcopy(damaged_j), W])
        return [True]
    gen_combinations(damaged_j, ind+1, J, alp, init_damaged_j, C_j, D_max, psi, rho, ans,pro)
    if ind not in damaged_j:
        damaged_j.append(ind)
        gen_combinations(damaged_j, ind+1, J, alp, init_damaged_j, C_j, D_max, psi, rho, ans,pro)
        damaged_j.remove(ind)
J = 5
z1 = [0.0 for i in range(J)]
C_j = [0,7,0,1,3]
D_max = 10
psi = 0.1
rho = 2
pro = [[0.3,0.2,0.2,0.1,0.15],[0.2,0.1,0.3,0.1,0.1],[0.2,0.3,0.2,0.1,0.1],[0.1,0.1,0.1,0.1,0.3],[0.15,0.1,0.1,0.3,0.2]]
D = [[0,1,2,1,3],[1,0,2,3,1],[2,2,0,1,1],[1,3,1,0,1],[3,1,1,1,0]]
```

```
n = 0.05
r = 0.05
alp = [[0 for x in range(J)] for y in range(J)]
      for i in range(J):
          for j in range(J):
              alp[i][j] = (r*(n**D[i][j]))

      damaged_j = [0,2]
      ans = []
      gen_combinations(damaged_j, 0, J, alp, deepcopy(damaged_j), C_j, D_max,
   psi, rho, ans,pro)
      ans.sort(key=lambda x: x[1])
      print ans
      print ans[0][0]
```

A.2. Code Explanation

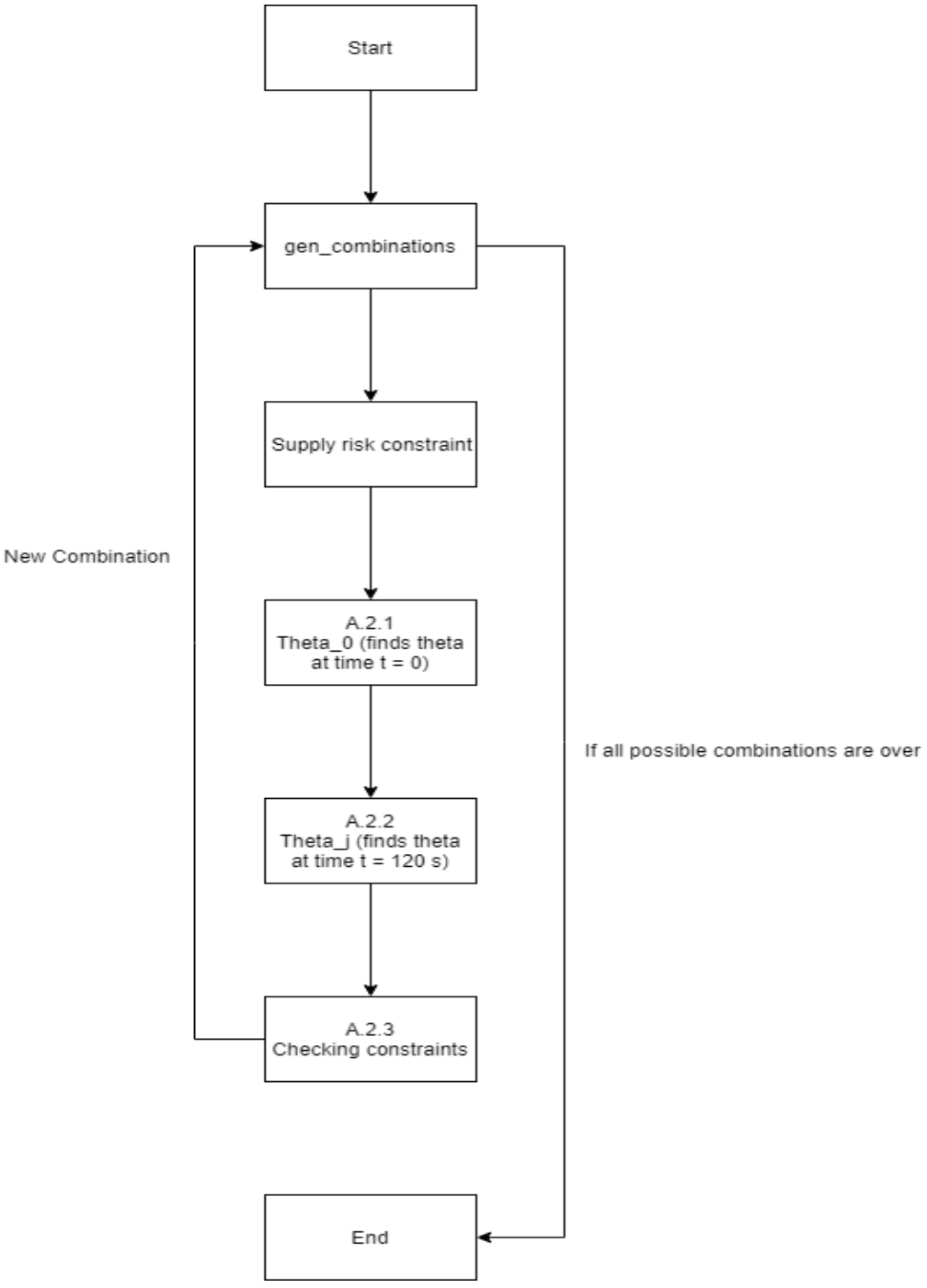

fig. A.1. Flow chart explaining the optimization code

A.2.1 Finding Initial Theta

The code below is used to find the θ j at t = 0 where damaged _ j is the EVCEs detected as compromised

```
def start_theta(damaged_j, pro):
    theta_0 = [0.0 for i in range(J)]
    for j in range(J):
        a1 = 1
        for i in range(J):
            if i in damaged_j and i!=j:
                a1 *= 1 - (0.1*(pro[i][j]))
        theta_0[j] = 1-a1
    print theta_0
    return theta_0
```

A.2.2 Finding Theta At Time t

The code below is used to find the θ j at time t

```
def gen_theta(damaged_j, theta_0, alp):
    theta_j = [0.0 for i in range(J)]
    z1 = [0.0 for i in range(J)]
    for i in range(J):
        if i not in damaged_j:
            theta_j[i] = theta_0[i]
    delta_t = 0.5
    time = 120
    # print damaged_j
    K = int(time/delta_t)
    for n in range(K+1):
        theta_new = [0.0 for i in range(J)]
        for j in range(J):
            if j not in damaged_j:
                a = (1 - theta_j[j])
                for i in range(J):
                    if i not in damaged_j and i != j:
```

```
                        a *= (1 - theta_j[i] * (alp[i][j]))
                #       print([i,j,alp[i][j],a])
                theta_new[j] = 1 - a
        if(n == K-1):
            z1 = theta_new
        theta_j = theta_new
    print "theta_j: ", theta_j
    return theta_j
```

A.2.3. Constraints

The below code is for constraints

```
# supply risk constraint
cx_sum = 0
a1 = 0
b1 = 0
c1 = 0
for j in range(J):
    if j not in damaged_j:
        cx_sum += C_j[j]
if cx_sum < (D_max * (1 - psi) - rho):
    return [False]
theta_0 = start_theta(damaged_j,pro)
theta_j = gen_theta(damaged_j, theta_0, alp)
for i1 in range(J):
    a1 = log(1 - z1[i1])
    for j1 in range(J):
        if(j1 not in damaged_j) and (j1 != i1):
            b1 += log(1 - (z1[j1] * alp[j1][i1]))
    c1 = b1+a1
    if (i1 not in damaged_j) and (c1 >= log(2-0.05)):
        return[False]
W = -1.0
for j in range(J):
    if j not in init_damaged_j:
        x_j = 0
        y_j = 0.0
        if j not in damaged_j:
            x_j = 1
            y_j = -log(1 - theta_j[j])
        W = max(W,y_j)
        # constraints
```

```
        if (y_j > x_j):
            return [False]
        if (y_j > -log(1 - theta_j[j])):
            return [False]
        if (y_j < (-log(1 - theta_j[j]) - (1 - x_j))):
            return [False]
        if (y_j < 0):
            return [False]
```

REFERENCES

[1] C. Carryl, M. Ilyas, I. Mahgoub, M. Rathod, "The PEV security challenges to the smart grid: Analysis of threats and mitigation strategies", *Proc. Int. Conf. Connected Veh. Expo (ICCVE)*, pp. 300-305, Dec. 2013.

[2] "Study of security attributes of smart grid systems—Current cyber security issues"2009, https://www.smartgrid.gov/files/Study_Security_Attributes_Smart_Grid_Systems _Current_ Cyber_200903.pdf

[3]"Electricity subsector cybersecurity risk management process", May 2012 https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

[4]https://ieeexplore.ieee.org/mediastore_new/IEEE/content/media/5165411/8497118/7930411/mousa1-2705188-large.gif

[5]https://www.dentelectricaz.com/dent-electric-blog/eleectric-vehicle-service-equipment-or-EVCE

[6]https://media.springernature.com/original/springer-static/image/art%3A10.1186%2F1687-1499-2014-223/MediaObjects/13638_2014_Article_1022_Fig6_HTML.jpg

[7]https://media.springernature.com/original/springerstatic/image/art%3A10.1186%2F1687-1499-2014-223/MediaObjects/13638_2014_Article_1022_Fig9_HTML.jpg

[8]https://media.springernature.com/original/springer-static/image/art%3A10.1186%2F1687-1499-2014-223/MediaObjects/13638_2014_Article_1022_Fig11_HTML.jpg

[9] M. Altunay, S. Leyffer, J. T. Linderoth, Z. Xie, "Optimal response to attacks on the open science grid", *Comput. Netw.*, vol. 55, no. 1, pp. 61-73, Jan. 2011.

[10] S. Cui et al., "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions", *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106-115, Sep. 2012.

[11] B. Sun, G. Yan, Y. Xiao, T. A. Yang, "Self-propagating mal-packets in wireless sensor networks: Dynamics and defense implications", *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1489-1500, 2009.

[12] S. Mousavian, J. Valenzuela, J. Wang, "A probabilistic risk mitigation model for cyber-attacks to PMU networks", *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 156-165, Jan. 2014.

[13] S. Mousavian, M. Erol-Kantarci, T. Ortmeyer, "Cyber attack protection for a resilient electric vehicle infrastructure", *Proc. IEEE Globecom Workshop Smart Grid Resilience*, pp. 1-6, Dec. 2015.